



January 26, 2023

Honorable Members of the Joint Technology Committee,

On behalf of the PII Advisory Group, I am pleased to present the study of the personally identifiable information (PII) as required by C.R.S § 24-37.5-122.

This group, established by the legislation and comprised of Government Data Advisory Board (GDAB) members and privacy experts, convened to fulfill the requirements to: a) study where PII is stored by state agencies throughout Colorado, b) study entities that have access to PII stored by state agencies, and c) determine the costs and processes necessary to centralize the storage and protection of (PII).

To determine PII locations and access, agencies completed a statewide data inventory, identifying data systems, data classifications and data stewards. The Advisory Group contracted with Gartner, Inc. to determine what would be required to centralize and protect PII. After interviewing 40+ key agency personnel and reviewing associated documents, Gartner concluded that statewide centralization of PII is not feasible due to legal concerns, cybersecurity risks, scale, cost, vendor ability and impact to operations. In addition, consolidating PII does not protect the application from being exploited by an attacker to exfiltrate PII. Gartner suggested several alternative technical options that could be pursued.

The Advisory Group has determined that we need more in-depth discovery and continued engagement with a contracted vendor to scope our current state prior to any prioritization or recommendation of the presented technical scenarios. Agencies have complex and diverse data ecosystems, with varying degrees of legal obligations, process maturity and resources that support systems critical to both the State of Colorado and its constituents. For future work the Advisory Group recommends:

- **Support Best Practices for PII - Priorities**
 - We have ongoing and planned initiatives aimed at increasing best practices. This work will be accomplished both collaboratively and by individual agencies. Additional resources have been requested in decision item R-05 The Road to Data Driven Decisions, that would support these initiatives
- **Potential consideration of PII Security Assessment Framework**
 - The Security Assessment Framework provided by Gartner is a concrete plan to address the security and privacy of PII. This could be implemented regardless of which (if any) technical option was chosen. As agencies are all at different levels of data maturity with different

resources, additional exploration and assessment of needed resources would be required.

- **Data Privacy** - Need for potential centralized and/or agency roles
 - Establishment of a state level role to create and manage a statewide privacy program to ensure that PII is managed according to best practices in compliance with all applicable privacy laws. This role could create policy and provide support to agencies
 - Establishment/Identification and funding of Data Privacy officers or similar roles at each agency. This may require additional FTE, though some agencies already have this position or job function.
- **Legal Review** - Study of potential laws/rules changes
 - The State needs further exploration of the legislative barriers to data sharing and consolidation and potential legislation to remediate these barriers, if appropriate.

We look forward to continuing the conversation around PII and working toward solutions that support the Digital Government Strategic Plan while creating the opportunity to provide our residents with the best possible services.

Sincerely,

A handwritten signature in black ink, reading "Amy Bhikha". The signature is fluid and cursive, with the first name "Amy" and last name "Bhikha" clearly distinguishable.

Amy Bhikha
Chief Data Officer

Approach

As stipulated in legislation, the PII Advisory Group was composed of Government Data Advisory Board (GDAB) members, with one representative per state agency, and privacy experts. These privacy experts represented the Office of Legal Counsel in the Governor’s Office, the Chief Information Security Office (CISO) in the Governor’s Office of Information Technology (OIT) and the OIT legislative liaison. This body convened to fulfill the requirements a) to study where personally identifiable information (PII) is stored by state agencies throughout Colorado, b) to study entities that have access to PII stored by state agencies, and c) to determine the costs and processes necessary to centralize the storage and protection of PII. To be good stewards of the \$193,000 provided by the fiscal note, as well as to maximize efficiency, the group looked to capitalize on and align with existing efforts undertaken by GDAB.

GDAB is a statutory committee, first established in 2009 and restructured in 2022, that meets a minimum of monthly with a mission to “Improve the efficiency and effectiveness of state government, Coloradan service delivery and policymaking by providing guidance and recommendations on how the state should govern and manage data and data management systems.” This group of agency data leaders, chaired by the Chief Data Officer, has worked to develop frameworks and templates that are geared to foster interoperability and alignment between state agencies. The past year, GDAB has been focused on meeting the legislative mandate for deliverables specified in HB21-1236. To accomplish this task, the GDAB took the innovative approach of forming subcommittees organized around the deliverables (Table 1). These subcommittees were made up of agency staff, with the goal of each agency having representation and input on each of the three subcommittees.

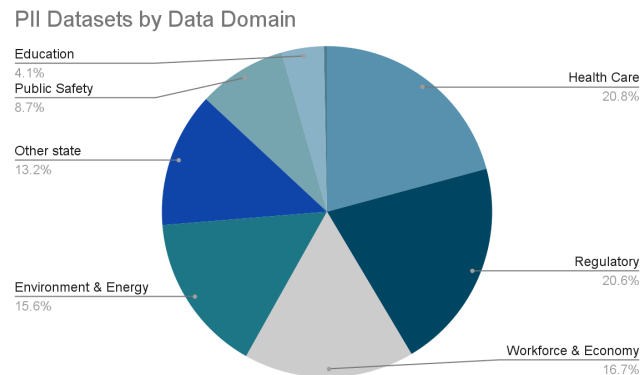
Table 1. GDAB Subcommittees and HB21-1236 Deliverables

| Data Inventory | Data Sharing | Data Governance |
|---|---|--|
| <ul style="list-style-type: none">• Data Inventory Scope & Requirements | <ul style="list-style-type: none">• Standard Inter-Government Data Sharing and Data Agreement<ul style="list-style-type: none">◦ CJIS Addendum• Data Sharing Policy and Procedure• List of Data Sharing Risks and Mediations• Data Sharing Standards and Terms | <ul style="list-style-type: none">• PII Definition• PII Protocol• Definition of Data Lifecycle and Accompanying Policy and Procedure• Data Retention Policy• Data Reconciliation Process |

It became apparent that the statewide Data Inventory, which was already underway, could also help to answer the questions related to where PII was stored and who had access to it. The Data Inventory subcommittee had designed a template, which was then used with each agency to help identify data systems, data types (including a PII indicator) and data stewards. The inventory was completed in November 2022. Over

1,822 data sets were inventoried and over 500 data stewards were identified. Of those, 987 data sets were determined to contain PII. For example, the RITS system, owned by the Colorado Department of Education (CDE) is the data set that contains student information and is used to assign the state student identifier. Healthcare, Regulatory and Workforce & Economy are the domains with the most collected PII. This sensitive data inventory is now housed within OIT. This was a monumental effort and is the most complete inventory the state has had thus far, though there have been previous efforts. As this information was manually produced and based on self-report, we must acknowledge its limitations. We are exploring plans to automate and maintain this data, contingent upon anticipated funds in FY23-24 that will allow for the purchase of a technology tool.

Figure 1. Datasets by Data Domain



To address the question of who has access to PII, we again used data gathered in the inventory process. For each data set, data stewards indicated how the data was classified in terms of ability to be released. Though some data sets are still under review, 733 data were classified as being potentially released (i.e., publicly available, released with restrictions, publicly requestable, sensitive). 216 have been classified as ineligible for release.

To begin to examine what would be needed around the centralization and protection of PII, the Advisory Group leveraged the funds provided by the fiscal note and in a competitive process awarded a contract to Gartner Consulting. Gartner is an industry leader, serving over 14,000 clients in over 100 countries.

In the course of this work Gartner produced four deliverables or report-outs that are included in appendices:

- Current State
- Target State
- Best Practices
- Security Assessment Framework
- Roadmap

Current State

To best understand the current state of PII and thus attenuate recommendations, Gartner entered into a discovery phase. Advisory Group members identified data experts from their respective agencies to be interviewed. OIT staff currently involved in projects related to identity were also debriefed. Gartner conducted 10 interviews with over 40 participants,

organized by data domain (Public Safety, Education, Health, Workforce & Economy, Regulatory, Environment & Energy, and Other State Government). Participants expressed some of the potential benefits of standardization, explained current configurations and talked about the challenges surrounding potential consolidation.

Table 2. Gartner Current State findings

| | Findings | Implications |
|--|--|--|
| 1. <i>Need for a Statewide Governance Model</i> | Some agencies maintain a data governance model and structure while others have elements of what a governance model may contain. Discrepancies among the agencies for how common data elements are housed, leveraged and shared can be rectified by a universal perspective for critical data. | A current set of varied approaches, data definitions and data models among the agencies demonstrates a need for a statewide PII data governance model. |
| 2. <i>Inconsistent Data Definitions</i> | Each agency and business unit leverages its own definition of what constitutes PII/PHI/FTI or other critical data elements as it relates to their specific organizational mission and business processes. Agency specific data and systems subsequently maintain differing levels of security, data usage and architecture due to these discrepancies. | Non-universal definitions of critical data elements and how their usage is to be governed can lead to potential data leaks or create data quality issues for agencies which share and consume data from partner agencies. |
| 3. <i>Need for a Statewide Data Model</i> | While there is a general belief that the mandates of the agency and program data needs are specific, there are commonalities at the data element level. Name, address, SSN and Colorado ID are potential examples that could knit Colorado agencies together. | A statewide data model is needed for consistent data sharing where necessary. This data model would enhance both reporting and data insight capabilities among agencies. It would also serve as a platform for a universal data definition standard. |
| 4. <i>Agency-Specific Data Requirements</i> | Each agency maintains specific timeframes for both data usage and storage. These depend on organizational mission and provided services. Various regulations and legal statutes are often agency-specific and can restrict how critical data is leveraged, shared and maintained within each agency. | Master Data Management strategies and solutions will require flexibility to ensure CO agency needs are upheld while limiting significant changes to existing processes or services provided. This will help ensure agency operations are not affected. |
| 5. <i>Singular Citizen Views</i> | Multiple agencies do share critical data with each other yet siloed data within agencies and across agencies limits staff's ability to create a singular Colorado citizen view to best serve their needs. | Siloed data architecture restricts some agencies from providing some needed government services or identifying users who should not have these services. This also restricts identification of citizens eligible for programs and understanding resident needs across agencies/program areas/service type. |
| 6. <i>Security Considerations</i> | Critical data sets require specific protections to ensure the safety and validity of the information that data houses. Just as with regulatory restrictions, the type of data and requisite security requirements vary significantly among agencies. These depend on their specific use cases and regulatory requirements. | Master and metadata management strategies will need to incorporate data-specific and agency-specific security practices and needs while still providing central systems for critical data. |

Gartner was provided additional documentation from the PII Advisory Group and agency experts. Provided information included: existing project documents (e.g., system architecture diagrams, data architecture diagrams, etc.), existing data inventories and system SAP Application Performance standards (SAPS), application data dictionaries and database diagrams, data specific process diagrams, system documentation (e.g., user guides, technical

documentation, architecture, interface specifications, etc.), standard operating procedures, policies and regulations related to PII or sensitive data elements.

Gartner was also briefed on ongoing efforts related to PII and identity management as outlined below:

GDAB Gartner was provided with the GDAB deliverables, which provide statewide guidance and are aimed at increased interoperability between state agencies, and the [GDAB website](#).

SIDMOD The State ID Module (SIDMOD) is a database software module that issues and tracks unique State Identification Numbers (State-IDs) and demographic information for clients applying for or receiving benefits. Current customers of SIDMOD include: Child Support Enforcement (ACSES), Medicaid, Food Assistance, Adult Financial and TANF programs (CBMS), Child Care Assistance Program (CHATS), and Children Youth and Families System (Trails).

IDXR OIT, in collaboration with the Lieutenant Governor's Office of eHealth Innovation (OeHI), is undertaking the development of a new statewide Individual Identity Cross-Reference (IDXR) service that provides state systems the ability to accurately identify individuals between and across other state systems when a unique identifier, such as social security or driver's license number, is not available. This service will be a critical infrastructure component for the establishment of a universal data interoperability platform, enabling the exchange of data on behalf of an individual between state systems that were not initially designed for that exchange but now have a need to do so.

Based on interviews and review of the PII Advisory Committee's provided documentation, Gartner summarized their six key findings and implications (Table 2). Though Gartner identified inconsistent definitions of PII across regulatory and statutory environments as a challenge, we would like to acknowledge that GDAB recently passed a statewide definition of PII and we are working to ensure that definition is deployed throughout the state. Within the Chief Data Office, we have also begun aligning data architects to data domains (Regulatory, Public Safety, Education, Health, Workforce & Economy, Energy & Environment, and Other State Agencies) that will help move us toward a statewide data model.

Target State

After analyzing the current state of PII at the state level, Gartner concluded that centralization of all PII is not feasible due to the potential for data breach, scale, cost, vendor ability and impact to operations.

The Advisory Group concurred with Gartner's findings and noted additional concerns:

- Legal & Regulatory: Differing legal mandates, rules, etc., across agencies
- Consent: Privacy impacts of centralization
- Security: Concern in scope for potential compromise of centralized location
- Data Ownership: Clarity on ownership and data-sharing agreements
- Procurement: Agencies are reliant on third-party software, with existing contracts and established programming that would require modifications
- Logistical: Non-consolidated agencies (e.g., Education, Judicial, SOS)

- **Priority:** Data strategy vs. agency priorities
- **Data Governance Maturity:** Differing data governance models and levels of maturity
- **Data Retention:** Differing policies by agency and usage
- **Cost:** Reiterating cost of restructure of current systems is prohibitive, including both technical and agency resources

Following analysis, Gartner provided four options to implement with PII throughout state agencies. Gartner recommended that Colorado pursue implementation of both Master Data Management and Metadata Management (Option 3). The approach, benefits and drawbacks of each option are presented in Table 3. Gartner noted that the recommendations could be implemented in a phased approach and should not necessarily be viewed as mutually exclusive. It should be noted that the projected costs listed below are capital outlay only and do not capture the expenses that would be borne by agencies, systems and processes in the level of effort for reconfiguration, including the potential for additional FTE.

Master Data Management System: A software application that would centralize a copy of information from each application with PII from all agencies, centralizing it at either the state level or within each agency, i.e., creating a “Golden Record” for each citizen that all agencies could use.

Examples:

- **Data Sharing and Reporting** - A constituent changed their address at the DMV. A central MDM repository ensures that other agencies like those that manage voter registration and tax information would have access to information about the address change.
- **Data Sharing and Reporting** - A Coloradan qualifies for the Colorado Homeless contribution income tax credit and is not enrolled in any housing or rental assistance programs. The Colorado Department of Local Affairs can identify eligible programs and notify the Colorado resident.

Metadata Management System: A software application that is used to enhance the usability, comprehension, utility or functionality of any other data point. This solution would track where PII data exists and who has access.

Examples:

- **Data Access** - All Colorado agencies using the metadata management system can see who has access to PII and where it exists across applications, they can also see where data is moving.
- **Data Sharing** - OIT can monitor how PII information is shared with third-party vendors and ensure the agreements with those vendors are being enforced effectively for not just applications with PII, but all applications within the system.
- **Lineage** - All agencies understand where the system of record exists, and can ensure changes there propagate to other systems.

Table 3. Gartner Potential Options

| | Option 1: Master Data Management (MDM) | Option 2: Metadata Management | Option 3: MDM & Metadata Management | Option 4: IDXR & Metadata Management |
|------------------|--|--|--|--|
| Approach | <ul style="list-style-type: none"> Start with implementing MDM (consolidation style) at each of the individual departments (golden record per department) As each organization's MDM matures consider implementation of MDM (consolidation style) at the state level (golden record for state) | <ul style="list-style-type: none"> Implement Metadata management (federated style) at each department As the state matures as an enterprise, consider implementation of the metadata management solution at the enterprise level. This will accommodate the metadata associated with other datasets & PII. | <ul style="list-style-type: none"> This is a combination of options 1 & 2 (Implement Master Data & Metadata Solutions in parallel). | <ul style="list-style-type: none"> Use existing IDXR architecture and expand based upon use-case classification or agency domain. Implement federated style of metadata management from option 2. |
| Benefits | <ul style="list-style-type: none"> Central source of cleansed, standardized and consolidated master data. Minimal footprint and impact to existing architecture. Provides the ability to define group and user level rights. Creates golden record at department and state levels. | <ul style="list-style-type: none"> Track the activities of data users to understand data usage, the most important data sets/records, related datasets and the nature of those relationships. Advanced insight will include data lineage and historical information as data records evolve over time among agencies. | <ul style="list-style-type: none"> Benefits of option 1 and 2 apply here. | <ul style="list-style-type: none"> IDXR is used to create a common citizen id across different systems / applications. Can track the activities of data users to understand data usage, the most important data sets/records, related datasets, and the nature of those relationships. |
| Drawbacks | <ul style="list-style-type: none"> This approach does not update the original source record for those consolidated data elements. Does not provide insights into the PII metadata (e.g., data usage, data access, etc.). | <ul style="list-style-type: none"> Only monitors the passive or active attributes of the datasets rather than the actual record. No golden PII customer record is created. | <ul style="list-style-type: none"> This approach does not update the original source record for those consolidated PII data elements. | <ul style="list-style-type: none"> IDXR functions like a registry MDM solution. This does not create a golden record. Unless expanded to and consolidated among all agencies, multiple instances of IDXR will be necessary each addressing specific agency data regulatory or policy restrictions. |

Table 4. Options Ability to Satisfy Legislative Requirements

| Legislative Requirements | | | | |
|-----------------------------|--|-------------------------------|-------------------------------------|--------------------------------------|
| | Option 1: Master Data Management (MDM) | Option 2: Metadata Management | Option 3: MDM & Metadata Management | Option 4: IDXR & Metadata Management |
| Identifies PII Requirements | Yes | Yes | Yes | Yes |
| Identifies PII Data Access | No | Yes | Yes | Yes |
| Centralization of PII Data | Yes | No | Yes | Partial Yes |
| 10-year Technical Cost* | \$40M – \$80M | \$10M – \$20M | \$50M – \$100M | \$35M - \$70M |

*Costs are only capital outlay and do not include costs borne by the agencies, including OIT. Please note the wide range of costs; additional scoping is required to true up these rough order of magnitude estimates.

In addition to the provided options, Gartner also generated a list of PII Controls (Fig 2) that should be in place prior to any major implementation. These components support appropriate PII best practices and would be beneficial regardless of which (or whether any) option was selected for implementation.

Figure 2. Required PII Controls

Required PII Controls Pre-Implementation Preparations

The following pre-implementation steps are necessary for ensuring that the State can implement one of these PII Data Management solutions. The below should be applied regardless of the solution chosen.

GOVERNANCE

Ensure that a single governance structure is established centrally for the project, with leads at the agency level and Colorado OIT. Currently, all Colorado agencies are federated with management of their PII and each agency owns their own data. Maintain the PII Advisory Board discussions to monitor project progress and discuss expansion.

CREATE A CONSISTENT DEFINITION OF PII ACROSS THE STATE

The Current State assessment identified that PII is still applied differently, with some agencies believing that an inclusion of one PII element makes a whole data set PII. Unify the view of items that do constitute PII from the GDAB definition of it (First and Last Name, SSN, etc.)

ADOPT THE GDAB DEFINITION OF PII TO DEPARTMENTAL POLICY

The Current State review identified that agencies are currently adapting the portions of the security policy that adheres to them. Apply a central security policy surrounding PII across agencies.

DATA & ANALYTICS STAFFING

Agencies have varying levels of data and analytics staffing and understanding. Enhance the maturity of the agencies by identifying a data steward either for the agency or by application for those with PII. Ensure the steward can speak to the quality of the data, ownership of it, how it's being used, etc.

PII TRAINING

Offer training to the agencies surrounding PII. Ensure they understand the definition, how to protect it, and who to notify if a question or issue occurs. Unify the application of the definition and protection of PII through training.

THIRD PARTY PII DATA OWNERSHIP

Ensure that a solution for security of PII data owned by third-parties is also considered as several agencies have this scenario. For data coming from third parties or being managed by third parties, governance is typically managed by Memorandums of Understanding (MOUs) or contract terms. Agencies have to take the data at their own risk. Ensure that each third-party application has the correct security parameters in place. From a list of 3rd party vendors, determine trust levels and how the data can be used.

24 RESTRICTED © 2022 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

PII Best Practices

Other states have implemented and experimented with centralized data approaches. To leverage what is known to work, Gartner provided example best practices (Fig 3). Using these best practices, we categorized our ongoing and planned initiatives (Fig 4). This validated that our efforts are aligned to best practices. To further contextualize this information for Colorado, Gartner outlined seven steps to structure the PII Program within agencies.

Structuring PII Data Program

1. Address Cultural Change
2. Educate the Agencies with a From...to...Approach
3. Define PII and Identify where it Exists
4. Determine a Governance Structure
5. Solution a Technology Platform
6. Define KPIs for the PII Program

Figure 3. Example State PII Best Practices

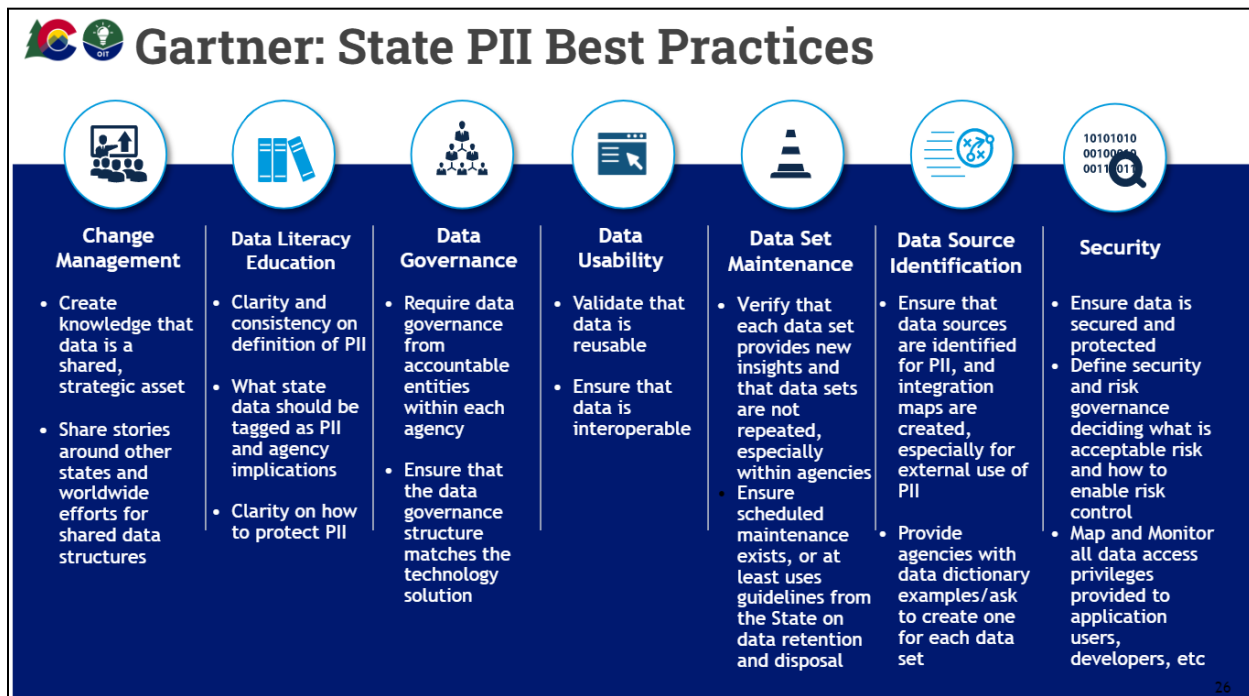
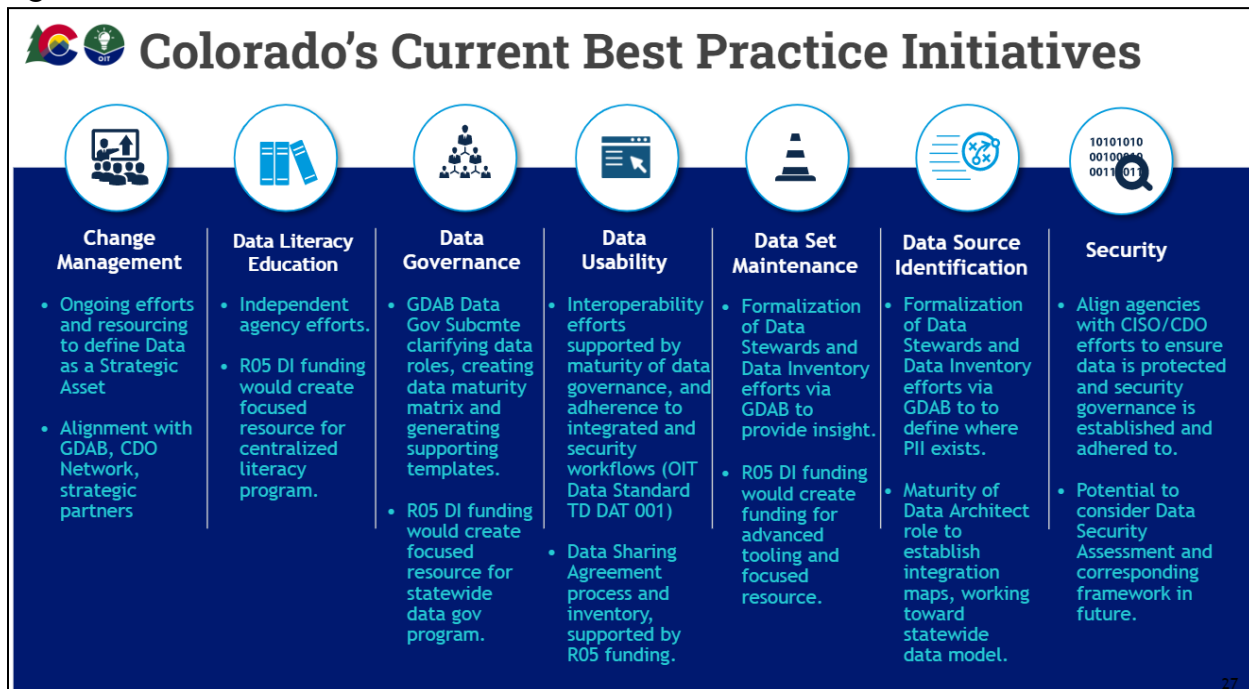


Figure 4. Colorado Best Practice Initiatives

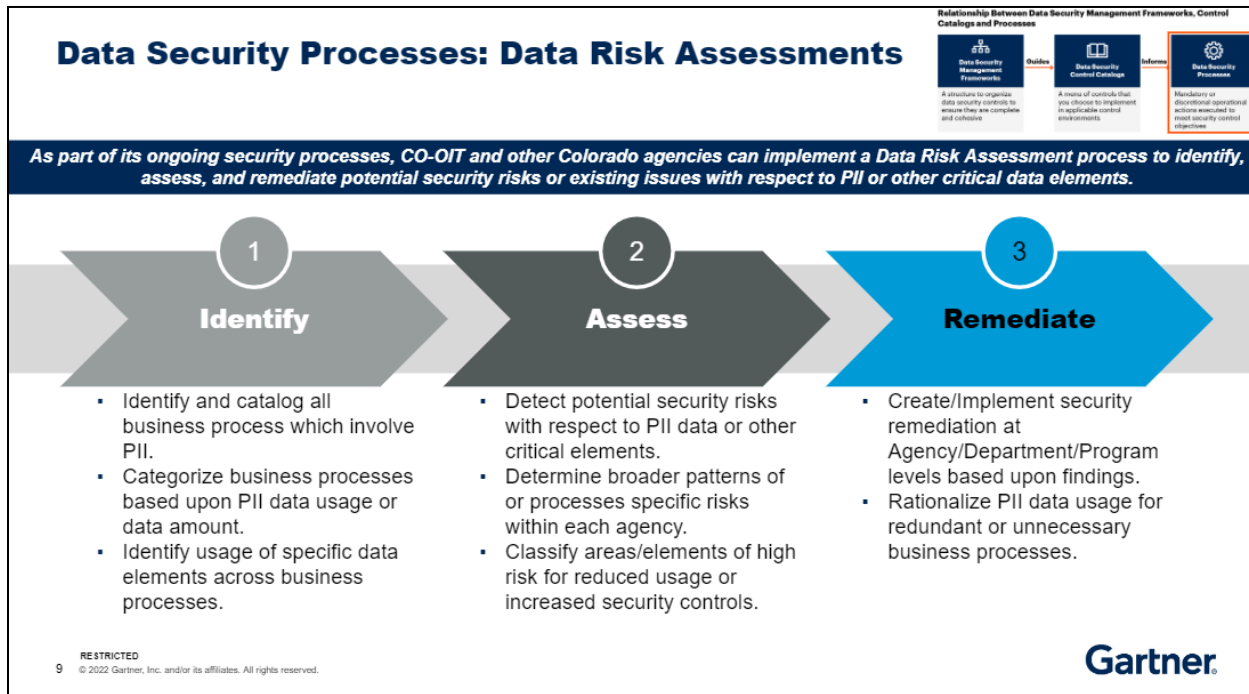


Security Assessment Framework

Recognizing that the desire to protect and secure data is underlying this project, Gartner also provided a Security Assessment Framework to evaluate the potential PII risk in agencies' current state and in potential centralized solutions. This process is designed to identify, assess and remediate risk (Fig 5). This framework assesses business processes related to PII across the domains of communication channels, process points and entry/exit points.

Implementation of this framework would represent substantial effort and coordination. We will require outside resources in the form of a contractor to help lay the groundwork and train staff on how to conduct these assessments.

Figure 5. Data Risk Assessments



PII Data Management Program: Initiative Roadmap

Gartner also provided a Roadmap to implement a technical solution to PII data management. The document outlines the three phases of implementation: 1) Plan, 2) Operationalize, 3) Mature. As the Advisory Group has determined they need more discussion and investigation of options, we would not be looking to move forward with this Roadmap immediately. The two year timeline provided is highly aggressive, which may not be practical. However, the step-by-step outline provides valuable information that could be useful if an implementation is chosen.

Conclusions, Recommendations & Next Steps

While Gartner has concluded that it is not feasible to centralize the collection and storage of PII, they presented several alternative options to consider. The PII Advisory Group is in full agreement that consolidation is not feasible. The PII Advisory Group has determined that more work and information gathering needs to occur before deciding on implementation feasibility of any of the suggested Gartner options.

To this end, we will continue to advance our maturity in how we manage our PII, as individual state agencies and collaboratively through GDAB. We will continue to leverage existing avenues and efforts, such as the work of GDAB, to improve our current state and ensure alignment with best practices. Any proposed statewide implementation would require additional scoping and understanding of our current

state data governance privacy and security, with particular focus on legal and procurement ramifications and required resources (financial and FTE).

There is consensus within the PII Advisory Group and the agencies this group represents that we are all interested in serving Coloradans effectively and efficiently and in alignment with the Digital Government Strategic Plan. Five of the enumerated strategies of the Digital Government Strategic Plan (Strategies 2, 3, 4, 5, and 6 as listed in Table 5.) are dependent on accurate, quality and timely data. This must be accomplished while taking into account appropriate security and privacy processes to protect our residents.

Table 5. Digital Government Strategic Plan Strategies

| |
|--|
| 1. Ensure all Coloradans have access to high speed internet |
| 2. Design around the life experiences of Colorado residents |
| 3. Use technology to improve service for residents |
| 4. Harness data to improve resident journeys and outcomes |
| 5. Cultivate analytics,business intelligence,and product leadership |
| 6. Bring best-in-class tools/technologies to how state agencies work |

For future work, the Advisory Committee recommends:

- **Support Best Practices for PII - Priorities**
 - As outlined in Figure 4, we have ongoing and planned initiatives aimed at increasing best practices. This work will be accomplished both collaboratively and by individual agencies. Additional resources have been requested in decision item R-05 The Road to Data Driven Decisions, that would support these initiatives.
- **Potential consideration of PII Security Assessment Framework**
 - The Security Assessment Framework provided by Garnter is a concrete plan to address the security and privacy of PII. This could be implemented regardless of which (if any) technical option was chosen. As agencies are all at different levels of data maturity with different resources, additional exploration and assessment of needed resources would be required.
- **Data Privacy - Need for potential centralized and/or agency roles**
 - Establishment of a state-level role to create and manage a statewide privacy program to ensure that PII is managed according to best practices in compliance with all applicable privacy laws. This role could create policy and provide support to agencies.

- Establishment/identification and funding of data privacy officers or similar roles at each agency. This may require additional FTE, though some agencies already have this position or job function.
- **Legal - Study of potential laws/rules changes**
 - The state needs further exploration of the legislative barriers to data sharing and consolidation and potential legislation to remediate these barriers, if appropriate.

At the conclusion of their study, Gartner has offered some suggested next steps. These next steps are aimed at helping us with the decision making and planning processes given the options they have presented. The PII Advisory Group has expressed the need for additional information and dialogue before moving forward with a technical option, thus these are not immediately actionable.

Gartner Proposed Next Steps:

1. Confirm legislative need and direction from the JTC given the four PII Data Management Solution options (i.e., remove options if possible given legislative direction).
2. Develop business cases for a PII Data Management Solution, identifying needs at each agency and confirming scope (including whether non OIT-consolidated agencies opt-in).
3. Complete a benefits analysis for the PII Data Management Solution project.
4. Discuss and determine viable deployment options from existing options.
5. Develop a detailed Total Cost of Ownership (TCO) model for selected viable options.
6. Identify top use cases for pilot initiatives.
7. Develop the TCO Model into a project budget and business case and request legislative approval.

In the more immediate future, OIT (specifically the Chief Data Office) can also consider incorporating other initiatives that can accelerate not just PII management needs but increase capabilities across agencies with respect to data management and usage:

1. Establish data governance standards and frameworks to be leveraged across agencies.
2. Develop a statewide data literacy program for agency personnel.
3. Define universal data security governance to establish acceptable levels of risk and how to enable risk control.
4. Continue to work on the initiatives around PII Best Practices as described in Figure 4.

This project provided an excellent opportunity for focused, collaborative discussions across the state agencies. Our partnership with Gartner provided the chance to receive feedback on our ongoing efforts from an industry leader. Their findings validate the ongoing work both in GDAB and at the agencies. They have also provided quality feedback on potential paths and considerations as we move forward. The Advisory Group is united in its commitment to providing excellent service to the residents of Colorado and we look forward to continuing the conversation around PII.

Appendices

| | |
|---|----------|
| PII Needs Analysis Report -Current State..... | Page 1 |
| PII Needs Analysis Report -Target State..... | Page 27 |
| Best Practices with PII..... | Page 112 |
| PII Needs Analysis Report -Security Assessment Framework..... | Page 132 |
| PII Data Management Program: Initiative Roadmap..... | Page 161 |
| Statewide Data Inventory Template..... | Page 184 |

PII Needs Analysis Report – Current State

Engagement #: 330079673 | Version 1
November 2022



COLORADO
Governor's Office of
Information Technology

| | | | |
|--|-----------|---|---------------|
|  | 01 | Engagement Overview and Document Purpose | Pages 3 – 5 |
|  | 02 | Current State Analysis - Summary | Pages 6 – 8 |
|  | 03 | Current State Analysis - Details | Pages 9 – 16 |
|  | 04 | Appendix – Interview Attendees | Pages 17 – 21 |

PII Needs Analysis Report Development

3 of 191

This Report summarizes the information Gartner obtained from the stakeholder interviews and establishes a high-level understanding of Colorado agency needs for managing PII data elements. Gartner will use this understanding of the current state to inform the target state and roadmap to evaluate potential Data Management strategies and solutions.

Summarize Discovery



Summarize Information from the Discovery Phase

- Provides a summary of Gartner's current assessment
- Gartner gathered information from interviews and State of Colorado documentation
- This document summarizes information from all sources of information into the key findings with additional details

Understanding Current State



Provide a High-Level Understanding of the State of Colorado's Current State

- Based on the interviews, and document reviews, Gartner has provided a high-level summary of current state opportunities, challenges, and considerations for data management initiatives

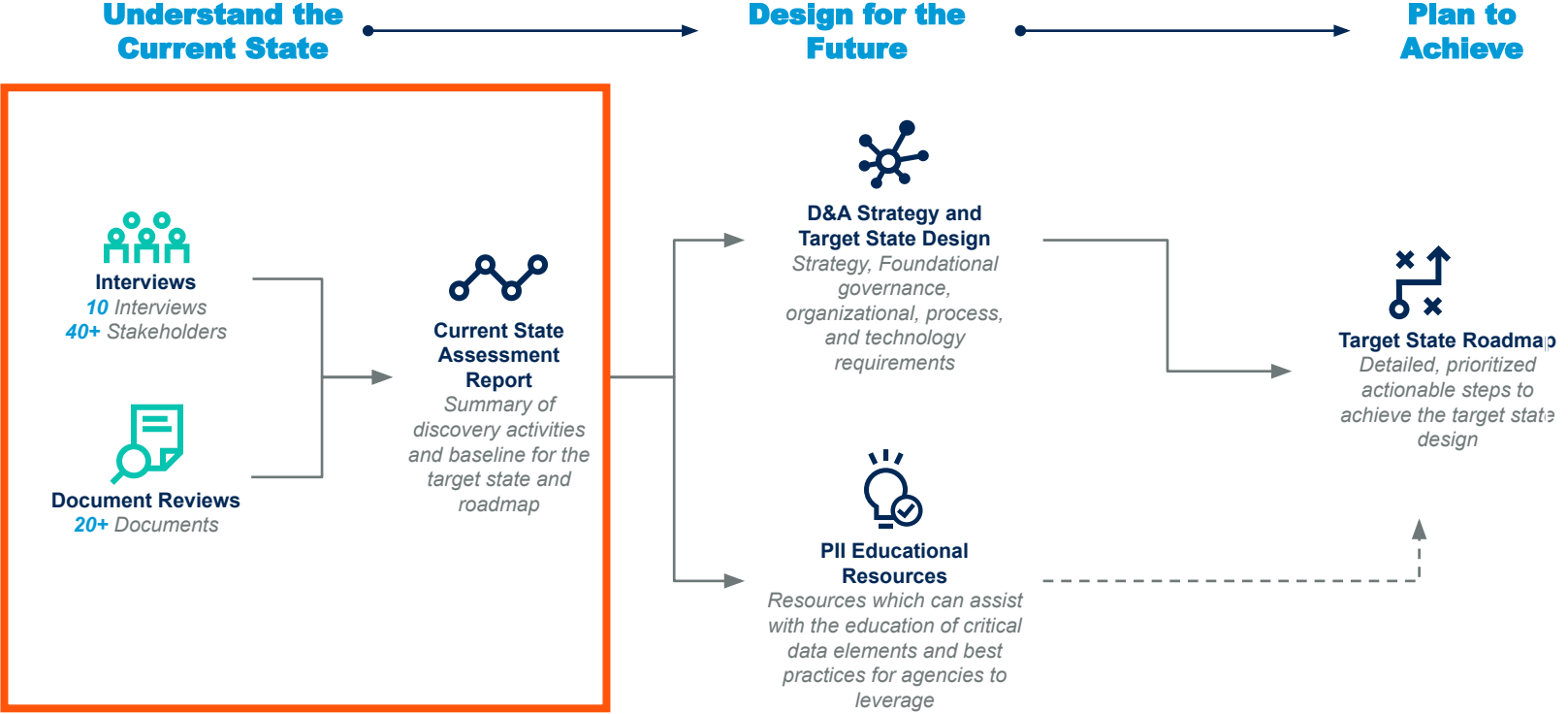
Define Specific Opportunities



Define Pain Points and Identify Proof of Concept Opportunities

- This document provides an overview of identified pain points which were captured during the interviews
- These pain points will inform future state needs surrounding the management of PII to align with Colorado agency and department expectations.

Gartner Engagement Overview



Focus of this Document

→

Primary Input

- - - - -

Supporting Input

Green icons denote actions | Blue icons denote deliverables

This engagement was initiated due to House Bill 21-1111

5 of 191

Legislator ask:

- Study **where personally identifiable information is stored** by state agencies throughout Colorado
- Identify entities that have **access** to personally identifiable information stored by state agencies
- **Determine the costs and processes** necessary to centralize the storage and protection of personally identifiable information
- Study to be completed and the advisory group is to present its findings and recommendations to the Joint Technology Committee(JTC) on or before **01/01/2023**
- Personally identifiable information means **information that may be used, along or in conjunction with any other information**, to identify a specific individual. Some examples can be found to the right.

Definition of Personally identifiable information from HB21-1111

Personally identifiable information means information that may be used, along or in conjunction with any other information, to identify a specific individual, including but not limited to:

- Name
- Date of birth
- Place of birth
- Social security number
- Tax identification number
- A password or passcode
- Official government-issued driver's license or identification card number
- Information contained in an employment authorization document
- Information contained in a permanent resident card
- Vehicle registration information
- License plate number
- Photograph
- Electronically stored photograph, or digitized image
- Fingerprint
- Record of a physical feature
- Physical characteristic
- Behavioral characteristic
- Handwriting
- Government passport number
- Health insurance identification number
- An employer, student, or military identification number;
- Financial transaction device
- School or educational institution attended;
- Source of income
- Medical information
- Biometric data
- Financial and tax records
- Home or work addresses or other contact information
- Family or emergency contact information;
- Status as a recipient of public
- Assistance or as a crime victim
- Race
- Ethnicity
- National origin
- Immigration or citizenship status
- Sexual orientation
- Gender
- Identity
- Physical disability
- Intellectual and developmental
- Disability
- Religion

Current State Analysis - Summary

There is a desire to leverage data amongst the Colorado agencies but significant challenges exist

7 of 104



Data is siloed within the department. It can be difficult to understand how Colorado citizens use department services.



We maintain very specific security restrictions for our PII data. I am concerned consolidating this information will introduce an attack surface



We leverage Data Sharing agreements with other agencies. How those agreements are structured can vary depending upon the data set or agency we are partnering with.



Pulling data from multiple sources to generate insight is challenging. There are issues with consistency of data quality when we use outside agency information.



We struggle with federal regulations for data because it varies so much from program to program.



Adding PII Data into PHI data makes it difficult to share other agencies.

Summary of Key Discovery Findings and Implications

8 of 191

1

**Need for a
State-wide
Governance
Model**

2

**Inconsistent Data
Definitions**

3

**Need for a
State-wide Data
Model**

4

**Agency Specific
Data
Requirements**

5

**Singular resident
Views**

6

**Security
Considerations**

Summary of Key Discovery Findings and Implications (Cont.)

9 of 191

Findings

Implications

1

Need for a State-wide Governance Model

Some agencies maintain a data governance model and structure while others have elements of what a governance model may contain. Discrepancies among the agencies for how common data elements are housed, leveraged, and shared can be rectified by a universal perspective for critical data.

A current set of varied approaches, data definitions, and data models among the agencies demonstrates a need for a State-wide PII data governance model.

2

Inconsistent Data Definitions

Each Agency and business unit leverages its own definition of what constitutes PII/PHI/FTI or other critical data elements as it related to their specific organizational mission and business processes. Agency specific data and systems subsequently maintain differing levels of security, data usage, and architecture due to these discrepancies.

Non-universal definitions of critical data elements and how their usage is be governed can lead to potential data leaks or create data quality issues for agencies which share and consume data from partner agencies.

Summary of Key Discovery Findings and Implications (Cont.)

10 of 191

Findings

Implications

3

Need for a State-wide Data Model

While there is a general belief that the mandates of the agency and program data needs are specific, there are commonalities at the data element level. Name, Address, SSN, Colorado ID are potential examples that could knit Colorado agencies together.

A state-wide data model is needed for consistent data sharing where necessary. This data model would enhance both reporting and data insight capabilities among agencies. It would also serve as a platform for a universal data definition standard.

4

Agency Specific Data Requirements

Each Agency maintains specific timeframes for both data usage and storage. These depend on organizational mission and provided services. Various regulations and legal statutes related to agency-specific data and can restrict how critical data is leveraged, shared, and maintained within each agency.

Master Data Management strategies and solutions will require flexibility to ensure State of CO agency needs are upheld while limiting significant changes to existing processes or services provided. This will help ensure agency operations are not affected.

Summary of Key Discovery Findings and Implications (Cont.) 1 of 191

Findings

Implications

5

Singular Resident Views

Multiple agencies do share PII and other data with each other yet siloed data within agencies and across agencies limits staff's ability to create singular Colorado resident view to best serve their needs.

Siloed data architecture restricts some agencies from providing some needed government services or identifying users who should not have these services. This also restricts identification of resident eligible for programs and understanding resident needs across agencies/program areas/service type.

6

Security Considerations

Critical data sets require specific protections to ensure the safety and validity of the information that data houses. Just as with regulatory restrictions, the type of data and requisite security requirements vary significantly among agencies. These depend on their specific use cases and regulatory requirements.

Master and Metadata Management strategies will need to incorporate data-specific and agency-specific security practices and needs while still providing central systems for critical data.

Current State Analysis – Details

– Details of Key Discovery Findings

Findings Details Overview

The following slides provide additional details for each of the 6 Key Discovery Findings.

Summary of Key Discovery Findings and Implications

| | Findings | Implications |
|---|--|--|
| 1 | Need for State-wide Governance Model Some agencies maintain a data governance model and structure while others have elements of what a governance model may contain. Discrepancies among the agencies for how common data elements are housed, leveraged, and shared can be rectified by a universal perspective for critical data. | A current set of varied approaches, data definitions, and data models among the agencies demonstrates a need for a State-wide PM data governance model. |
| 2 | Inconsistent Data Definitions Each Agency and business unit leverages its own definition of what constitutes PII/PHFI or other critical data elements as it related to their specific organizational mission and business processes. Agency specific data and systems subsequently maintain differing levels of security, data usage, and architecture due to these discrepancies. | Non-universal definitions of critical data elements and how their usage is to be governed can lead to potential data leaks or create data quality issues for agencies which share and consume data from partner agencies. |
| 3 | Need for a State-wide Data Model While there is a general belief that the mandates of the agency and program data needs are specific, there are commonalities at the data element level. Name, Address, SSN, Colorado ID are potential examples that could knit Colorado agencies together. | A state-wide data model is needed for consistent data sharing where necessary. This data model would enhance both reporting and data insight capabilities among agencies. It would also serve as a platform for a universal data definition standard. |
| 4 | Agency Specific Data Requirements Each Agency maintains specific timelines for both data usage and storage. These depend on organizational mission and provided services. Various regulations and legal statutes are often agency specific and can restrict how critical data is leveraged, shared, and maintained within each agency. | MDM strategies and solutions will require flexibility to ensure CO agency needs are upheld while limiting significant changes to existing processes or services provided. This will help ensure agency operations are not affected. |
| 5 | Singular Citizen Views Multiple agencies do share critical data with each other yet siloed data within agencies and across agencies limit staff's ability to create singular Colorado citizen view to best serve their needs. | Siloed data architecture restricts some agencies from providing some needed government services or identifying users who should not have these services. This also restricts identification of citizens eligible for programs and understanding resident needs across agency/program awareness type. |
| 6 | Security Considerations Critical data sets require specific protections to ensure the safety and validity of the information that data houses. Just as with regulatory restrictions, the type of data and requisite security requirements vary significantly among agencies. These depend on their data and their departmental objectives. | Master and Meta Data Management strategies will need to incorporate data specific and agency specific security practices and needs while still providing central systems for critical data. |

1 Finding

Output statements based on Gartner's analysis of the evidence

The key findings represent a synthesis of information the Gartner team received multiple times in interviews, document reviews, or based on both.

2 Evidence

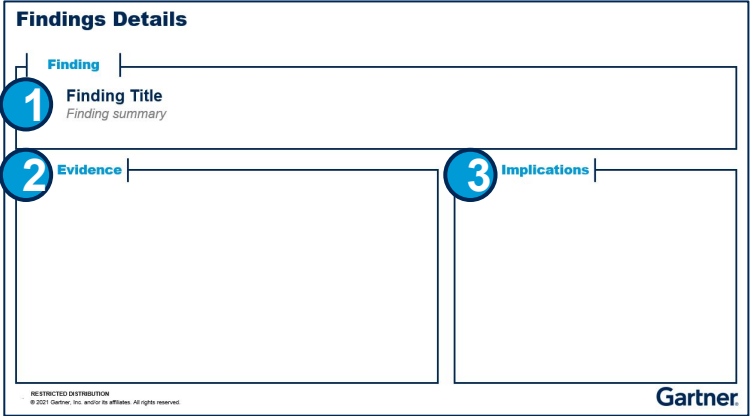
Information to support the finding

The list of evidence points supporting the statements of fact from Gartner's discovery period to support the finding.

3 Implications

Gartner's judgment regarding the impact of the finding

The implications are the potential effects, barriers or costs of how the finding may impact Colorado OIT today and tomorrow based upon its MDM strategy and approach. These implications are not a one-to-one mapping or recommendation but rather awareness for how the findings may impact the design of target state.



Findings Details (1 of 6)

Finding

1

Need for a state-wide data governance model

Some Colorado agencies maintain a data governance model and structure while others have elements of what a governance model may contain. Discrepancies among the agencies for how common data elements are housed, leveraged, and shared can stem from a lack of a universal perspective for what is personally identifiable information (PII) data and how to manage it.



Evidence

- ❑ Agencies each maintain varying levels of formal documented data governance standards with their respective agencies and programs e.g., OIT, The Governor's Office of eHealth Innovation (OeHI), Colorado's Department of Health Care Policy and Financing (HCPF), and Colorado's Department of Human Services (CDHS) have implemented the State ID Module System (SIDMOD) to track State-IDs across multiple systems (Automated Child Support Enforcement System (ACSES), Child Care Automated Tracking System (CHATS), Colorado Benefits Management System (CBMS)/Program Eligibility & Application Kit (PEAK), and Child Welfare Case Management System (Trails)) and create a common client identifier and improve data quality.
- ❑ Several agencies rely predominantly on key personnel to ensure specific data policies (e.g., retention, sharing, etc.) are implemented and maintained.
- ❑ Many agencies or programs are relatively early in their respective data management journey's and do not maintain an understanding of what information they manage.
- ❑ Some agencies do not have complete insight into where PII data exists across the various systems / applications that support them



Implications

- ❑ Aspects of data management such as regulatory restriction (e.g. Family Educational Rights and Privacy Act - FERPA, SNAP Data Disclosure, etc.) data retention, data quality, and data sharing, are domains which each agency approached uniquely. This creates a wide spectrum of diverse levels of PII data management approaches across agencies.
- ❑ Data Governance provides the standards and policies for PII data e.g., creating a unified system of record and a common identifier for a resident or non-resident across the different systems within a department or even across departments and agencies. The inability to do this results in individual agencies lacking a single holistic view of the resident or non-resident they are serving.

Finding

2

Inconsistent Data Definitions

Each Agency and business unit leverages its own definition of what constitutes Personally Identifiable Information (PII), Personal Health Information (PHI) or Federal Tax Information (FTI) or other critical data elements as it related to their specific organizational mission and business processes. Agency specific data and systems subsequently maintain differing levels of security, data usage, and architecture due to these discrepancies.



Evidence

- ❑ Each agency maintains its own unique definition of what constitutes PII/PHI/FTI or other critical data elements it manages
- ❑ While several agencies understand which information is managed within their infrastructures, how that information is classified and the subsequent policies which apply vary from agency to agency



Implications

- ❑ With inconsistent definition of critical data, agencies apply differing rules and policies even to common data elements.
- ❑ A lack of data literacy skills can cause a lot of damage to your data. Employees may store and / or share wrong information as they don't understand the data classification of sensitive PII/PHI/FTI data

Findings Details (3 of 6)

Finding

3 Lack of a state-wide data model

While there is a general belief that the mandates of the agency and program data needs are specific, there are commonalities at the data element level. Name, Address, SSN, Colorado ID, Colorado DMV ID, SIDMOD are potential examples that could knit Colorado agencies together.

Evidence

- ❑ Many of the agencies maintain within their respective infrastructures or consume PII elements as part of data sharing with external partners. Many of the elements in question are common (Name, SSN, Physical Address, Phone Number, Colorado DMV ID, etc.).
- ❑ These specific elements often serve as the data index for joining data sets together for analysis or garnering specific insight.

Implications

- ❑ A state-wide Master Data Management strategy, needed for data management and sharing, needs to be based on a state-wide data model, that includes identification of individuals based on common data elements.
- ❑ Lack of a data model impedes data definition standardization and allows for Colorado agencies to have various classifications of PII data.
- ❑ In the absence of a state-wide data model there will be challenges related to collaborating with agencies to obtain data for analytics to identify potential stolen identities used in cases of fraud, waste and abuse. An important component of this is having robust data sharing and data security agreements in place that will provide access to information across agencies.

Findings Details (4 of 6)

Finding

4

Agency Specific Requirements

Each Agency maintains specific timeframes for both data usage and storage. These depend on organizational mission and provided services. Various regulations and legal statutes related to agency-specific data and can restrict how critical data is leveraged, shared, and maintained within each agency.



Evidence

- ❑ Each agency and department interviewed adheres to specific regulations, legal statutes, or policies which govern critical data use, management, and sharing.
- ❑ There are overlaps for how critical PII data usage or management is restricted by these regulations or policies. GDAB Risks and Barriers document captures the primary barriers identified to data sharing and the associated risk to violating the law / agreement
- ❑ There is not a comprehensive set of regulations or policies which govern critical data elements which each Agency/department must adhere to, i.e., what defines Personally Identifiable Information. However, GDAB has adopted the PII definition from State of CO Statutes that states:

"PII means information which can reasonably be used to identify, contact or locate an individual, either alone or in combination with other information. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual".



Implications

- ❑ Multiple federal laws regarding the protection of PII data often have different terms or requirements for maintaining or using PII data and need to be taken into account while formulating a state-wide PII data strategy.
- ❑ Because of these multiple requirements, the State will need to ensure that agencies are actively involved in the creation of a statewide PII management strategy and selection of a potential vendor solution for managing PII.

Findings Details (5 of 6)

18 of 191

Finding

5 Singular Resident View

Multiple agencies share PII and other data with each other, yet siloed data within agencies and across agencies limits staff's ability to create a singular Colorado resident view to best serve their needs.

Evidence

- ❑ Across the agencies, there are several use-cases or scenarios where agencies would benefit from having access to specific external data sets to generate insight on resident needs, identify potential residents for specific programs and potentially improve government services.
- ❑ Certain agencies attempt to resolve this issue by aggregating some of the PII data across programs or agencies to create a unified “resident view” of individuals yet this capability is typically limited to just within agencies.
- ❑ Agencies struggle with garnering access to the specific data in question either due to regulation, policy restriction, or lack of formal data sharing agreements.
- ❑ Within agencies, program areas struggle to share information among business groups to perform their required data and analysis and scheduled reporting

Implications

- ❑ In the absence of an end-to-end view of the resident within a department or across agencies, the State has limited ability to become resident-centric. A resident-based view would allow agencies to track the impact of services as well as identify new services and programs that would benefit them.
- ❑ A 360-degree resident view would provide transparency and bridge data silos. This view would also enable agencies to collaborate and make better decisions. This view would enable the State to work towards ensuring residents are notified about the programs and services for which they are eligible.

Findings Details (6 of 6)

Finding

6

Security & Privacy Considerations

Critical data sets require specific protections to ensure the safety and validity of the information that data houses. Just as with regulatory restrictions, the type of data and requisite security requirements vary significantly among agencies. These depend on specific use cases and regulatory requirements.



Evidence

- ❑ PII data is stored across multiple different systems, spreadsheets and within hard copies of documents. Not all agencies have a through understanding of where Personally Identifiable Information (PII), Personal Health Information (PHI) and Federal Tax Information (FTI) is stored.
- ❑ The broad definition of PII creates security and privacy challenges for agencies collecting, processing and storing PII. Each department is responsible for determining what defines PII in its jurisdiction and which statutes are in scope for compliance. There is no singular governance body or set of laws that covers the privacy of PII / PHI /FTI at the federal level. Instead, there are a mix of groups and a mix of laws like HIPAA, FERPA, COPPA, etc. Adding State level legislation or policies, adds to the complexity on how to apply security and privacy policies.
- ❑ Agencies agree upon the common PII elements (Name, SSN, Physical Address, Phone Number, Colorado DMV ID, etc.). When this data is combined with department specific data or protected data sets the complete data set is considered PII. This can lead to enhanced protections and regulatory compliance above that afforded with PII.
- ❑ State employees are provided with generalized cybersecurity training. Many agencies provide additional data training e.g. HIPAA obligations for privacy.
- ❑ There is a lack of tracking on repositories containing PII data



Implications

- ❑ Data breaches, misuse of data, data leakage, inappropriate data sharing etc., can occur due to negligent or accidental exposure of sensitive data. This problem can be addressed by:
 - ❑ Learning what data exists, where the data is stored and how it is used
 - ❑ Providing regular employee training related to security policies, regulatory compliance and providing an understanding what data is at risk of being stolen or misused due to its sensitive nature
 - ❑ Protecting PII data that is in transit and at rest. For data at rest it is important to understand the sensitivity of the data and where it resides. This data is only as secure as the infrastructure that supports it. For data in transit consider restrict user access by role, encryption etc.
- ❑ In the case of a security breach, many of the repositories do not have the capability to track exfiltration, resulting in PII data being compromised

Appendix

– Interview Attendees

Detailed Requirements Workshops Participants

21 of 191

Gartner and Colorado OIT conducted the following interview sessions between 10/28 and 11/10 to collect information regarding detailed requirements:

| Date | Time (MST) | Group | State of Colorado Attendees |
|------------|------------|-----------------------|---|
| 10/28/2022 | 11am | Education | Craig Kim - OIT Katherine Hochevar - OIT Amy Bhikha - OIT Dennis Loerzel - CDE Melissa Peterson - CDE Adam Kanter – DHE Michael Vente - CDHE Kevin Smith – CDE |
| 10/31/2022 | 11am | Workforce and Economy | Craig Kim - OIT Amy Bhikha - OIT Katherine Hochevar - OIT Thomas Kulp - CDLE James Wiegand - DOLA Amanda Neal - CDLE Bryce Jones – State |
| 11/10/2022 | 2.30pm | IDXR Deep Dive | Craig Kim - OIT Amy Bhikha - OIT Katherine Hochevar - OIT Eric Hoffman - OIT Contractor |

Detailed Requirements Workshops Participants (Cont.)

22 of 191

Gartner and Colorado OIT conducted the following interview sessions between 10/28 and 11/10 to collect information regarding detailed requirements:

| Date | Time (MST) | Group | State of Colorado Attendees |
|------------|------------|-------------------------------|---|
| 11/02/2022 | 1pm | Public Safety | Craig Kim - OIT Katherine Hochevar - OIT Amy Bhikha - OIT Michael Bruno - DMVA Chris Andrist - State Michael Gaenzle – State Jack Reed – CDPS |
| | 2pm | Environment and Eng. (Part 1) | Craig Kim - OIT Katherine Hochevar - OIT Amy Bhikha – OIT Eric Lowe – State Rachel Davis – CDOT Kristi Gitkind – State |

Detailed Requirements Workshops Participants (Cont.)

23 of 191

Gartner and Colorado OIT conducted the following interview sessions between 10/28 and 11/10 to collect information regarding detailed requirements:

| Date | Time (MST) | Group | State of Colorado Attendees |
|------------|------------|--------|--|
| 11/03/2022 | 11am | Health | Craig Kim - OIT Katherine Hochevar - OIT Amy Bhikha – OIT Jane Wilson - State Joni Koenig - CDPHE Michael Martinez - CDHS Lyn Snow - State Roberta Lopez - State Nourou Gaiya - State Amelia Larsen – State Eric Hoffman – State |
| | 3pm | OIT | Craig Kim - OIT Katherine Hochevar - OIT Amy Bhikha - OIT John Sarica - OIT Contractor Ray Yepes - OIT Thad Batt - OIT Amy Bhikha - OIT Katherine Hochevar - OIT Jane Rosenthal - OIT Milo Knezevic - OIT Bruno Silva - OIT Stephen Petty - OIT |

Detailed Requirements Workshops Participants (Cont.)

24 of 191

Gartner and Colorado OIT conducted the following interview sessions between 10/28 and 11/10 to collect information regarding detailed requirements:

| Date | Time (MST) | Group | State of Attendees |
|------------|------------|-------------------------------|---|
| 11/04/2022 | 9am | Environment and Eng. (Part 2) | Craig Kim - OIT Katherine Hochevar - OIT Amy Bhikha - OIT Amy Klene – DNR Hollis Glenn – CDA Windi Padia - DNR |
| | 11.30am | Regulatory | Craig Kim - OIT Katherine Hochevar - OIT Amy Bhikha - OIT Lauren Hamby – DORA Laura Koeneman – State Mari Villagomez - DORA Amber Egbert - DOR Sarah Clark - DPA Marisol Larez - DORA Ronne Hines – State Eric Hurley - State |
| | 3pm | State Government | Rich Schliep, CTO, Secretary of State Trevor Timmons, CIO , Secretary of State Jason Harris, Judicial Sherry Foco, Judicial |

Detailed Requirements Workshops Participants (Cont.)

25 of 191

Gartner and Colorado OIT conducted the following interview sessions between 10/28 and 11/10 to collect information regarding detailed requirements:

| Date | Time (MST) | Group | State of Attendees |
|------------|------------|-----------------|--|
| 11/09/2022 | 2.30pm | Final Interview | Craig Kim - OIT - organizer Valeri Limes - CDEC Bill Waggoner- COAG Dalia Ritvo - COAG Marcia Bohannon - CDE Amy Bhikha - OIT Katherine Hochevar - OIT |
| 11/10/2022 | 2.30pm | IDXR Deep Dive | Craig Kim - OIT Amy Bhikha - OIT Katherine Hochevar - OIT Eric Hoffman - OIT Contractor |

Bharat Bagaria

Expert Partner
Gartner Consulting
Phone: +1 916 210 0907
Email: bharat.bagaria@gartner.com

Chelsea Wyatt

Senior Managing Partner
Gartner Consulting
Phone: +1 303 590 8599
Email: chelsea.wyatt@gartner.com

Farhat Naweed

Senior Director
Gartner Consulting
Phone: +1 475 685 5848
Email: farhat.naweed@gartner.com

Nikhil Nayak

Associate Director
Gartner Consulting
Phone: +1 916 213 7447
Email: nikhil.nayak@gartner.com

Lauren Talyor

Account Executive
Gartner
Phone: +1 205 837 3693
Email: lauren.talyor@gartner.com

PII Needs Analysis Report – Target State

Engagement #: 330079673 | Version 1



COLORADO
Governor's Office of
Information Technology

Contents

28 of 191



01

Engagement Overview and Document Purpose

Pages 3 - 6



02

Target State and ROM

Pages 7 – 19



03

Implementation Considerations

Pages 20 – 25



04

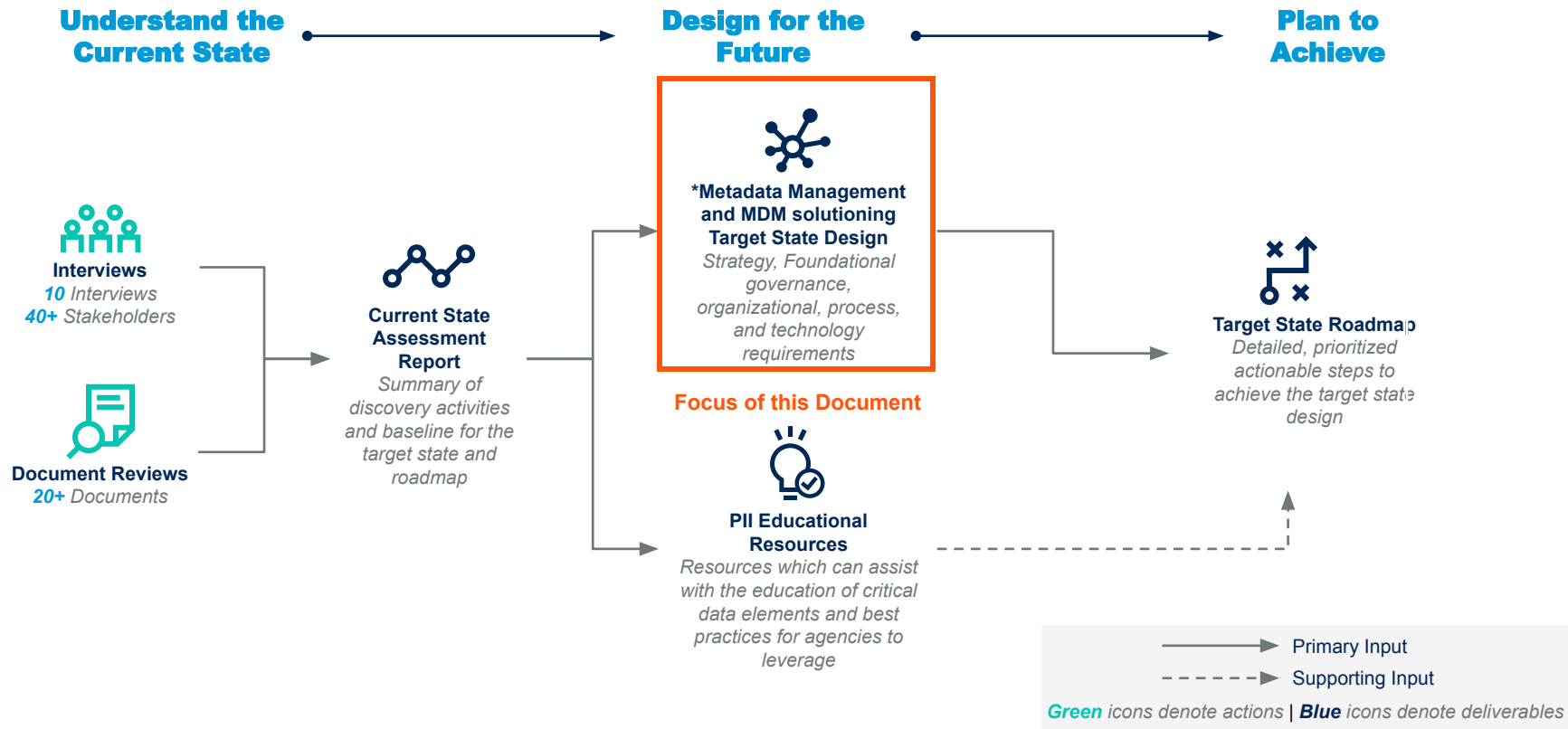
Appendix

Pages 26 – 84

Executive Overview

Gartner Engagement Overview – PII Solution Architecture

30 of 191



This engagement was initiated to address House Bill 21-1111

31 of 191

Legislator ask:

CDO to create and lead the PII Advisory Group to:

- Study **where personally identifiable information is stored** by state agencies throughout Colorado
- Identify entities that have **access** to personally identifiable information stored by state agencies
- **Determine the costs and processes** necessary to centralize the storage and protection of personally identifiable information
- Study to be completed and presented to the Joint Technology Committee(JTC) on or before **01/01/2023**
- Personally identifiable information means **information that may be used, along or in conjunction with any other information**, to identify a specific individual. Some examples can be found to the right.

Personally identifiable information

Personally identifiable information means information that may be used, along or in conjunction with any other information, to identify a specific individual, including but not limited to:

- Name
- Date of birth
- Place of birth
- Social security number
- Tax identification number
- A password or passcode
- Official government-issued driver's license or identification card number
- Information contained in an employment authorization document
- Information contained in a permanent resident card
- Vehicle registration information
- License plate number
- Photograph
- Electronically stored photograph, or digitized image
- Fingerprint
- Record of a physical feature
- Physical characteristic
- Behavioral characteristic
- Handwriting
- Government passport number
- Health insurance identification number
- An employer, student, or military identification number;
- Financial transaction device
- School or educational institution attended;
- Source of income
- Medical information
- Biometric data
- Financial and tax records
- Home or work addresses or other contact information
- Family or emergency contact information;
- Status as a recipient of public
- Assistance or as a crime victim
- Race
- Ethnicity
- National origin
- Immigration or citizenship status
- Sexual orientation
- Gender
- Identity
- Physical disability
- Intellectual and developmental
- Disability
- Religion

Gartner understands the Colorado legislature desires to provide greater security surrounding PII data elements

2210



The Colorado Legislature has commissioned this study to understand an overall approach, potential options, and rough order or magnitude costs to centralize PII or other critical data assets.



Gartner's assessment indicates complete centralization of PII or other critical data assets is unfeasible at this time for the following reasons:

1. **Scale** - Consolidation of PII data assets into a singular source would require major modification or redevelopment of hundreds of applications across the 29 Colorado agencies
2. **Unsupported by Vendors** - COTS vendors would not be able to support this type of uplift due to the overall scale of the data elements
3. **Cost Prohibitive** - This type of change is cost prohibitive with costs great than \$1 Billion due to the modification of all the other applications required
4. **Impact to Operations** - The change would not allow for operational business to function at most of the Colorado agencies, if not all
5. **Data Breach** - Data breaches at the application layer are a pathway for external attackers, or insiders to achieve their goal of gaining access to sensitive data. Traditional approach to security won't work as you need visibility across the environment and to understand the lateral movements that happen during a breach

RESTRICT

Target State and ROM

Master Data Management (MDM) and Metadata Management 14 of 191

Below are the two directions for managing Personally Identifiable Information (PII) that the State of Colorado can consider.



MDM MANAGEMENT

Master Data Management System: A software application that would centralize a copy of information from each application with PII from all agencies, centralizing it at either the State level or within each agency, i.e. creating a “Golden Record” for each citizen that all agencies could use.

EXAMPLES

- **Data Sharing and Reporting** - A constituent changed their address at the DMV. A central MDM repository ensures that other agencies like those that manage voter registration and tax information would have access to information about the address change.
- **Data Sharing and Reporting** - A Coloradoan qualifies for the Colorado Homeless contribution income tax credit and is not enrolled in any housing or rental assistance programs. The Colorado Department of Local Affairs can identify eligible programs and notify the Colorado citizen.



METADATA MANAGEMENT

Metadata Management System: A software application that used to enhance the usability, comprehension, utility or functionality of any other data point. This solution would track where PII data exists and who has access.

EXAMPLES


- **Data Access** - All Colorado agencies* using the metadata management system can see who has access to PII and where it exists across applications, they can also see where data is moving.
- **Data Sharing** - OIT can monitor how PII information is shared with third-party vendors and ensure the agreements with those vendors are being enforced effectively for not just applications with PII, but all applications within the system.
- **Lineage** - All agencies understand where the system of record exists, and can ensure changes there propagate to other systems. A public health patient's name change in their patient portal could propagate to other systems if Colorado Health and Human Services structured it this way.

CO-OIT has 5 solution options to consider for meeting the needs of House Bill 21-1111

35 of 191



Notes:

- Options 1 through below would meet some of the requirements of HB21-1111
- While PII and critical data elements are the primary focus, these options can be leveraged for other datasets as well
- For options 1 through 4, no option is required to precede another, and each can be evaluated individually
- Option 5 would provide insight into security processes and tools necessary for each agency business process containing PII data

| | Option 1: Master Data Management (MDM) | Option 2: Metadata Management | Option 3: MDM & Metadata Management | Option 4: Entity Resolution & Metadata Management | Option 5: PII Process Management |
|---|--|---|---|--|---|
|  Approach | <ul style="list-style-type: none">▪ Start with Implementing MDM (Consolidation Style) at each of the individual Department (Golden record per department)▪ As each organization's MDM matures consider implementation of MDM (Consolidation Style) at the State level (Golden record for State) | <ul style="list-style-type: none">▪ Implement Metadata management (Federated Style) at each department▪ As the State mature as an enterprise, consider implementation of the metadata management solution at the enterprise level. This will accommodate the metadata associated with other data sets as well as PII | <ul style="list-style-type: none">▪ This is a combination of options 1 & 2 (Implement Master Data & Metadata Solutions in parallel) | <ul style="list-style-type: none">▪ Use existing IDXR architecture and expand based upon use-case classification or agency domain▪ Implement federated style of metadata management from option 2 | <ul style="list-style-type: none">▪ Complete a security assessment of business processes with PII elements▪ Implement bi-annual security process review to track progress of security gap mitigation▪ Create a PII Data Sharing Policy within OIT for adoption across other agencies▪ Create/Refine a Data Sharing Agreement for agency adoption |

















































Gartner evaluated each option's ability to fulfill requirements of HB21-111

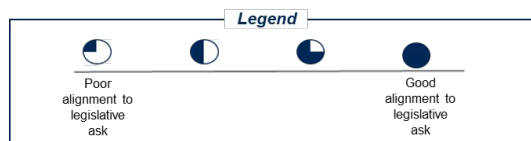
36 of 191

| Legislative Requirement | Option 1: MDM | Option 2: Metadata Management | Option 3: MDM & Metadata Management | Option 4: Entity Resolution & Metadata Management | Option 5: PII Process Management |
|--|---|--|--|--|--|
| Identifies PII Data Locations | Yes | Yes | Yes | Yes | Yes |
| Identifies PII Data Access | No | Yes | Yes | Yes | Partial Yes |
| Centralization of PII Data | Yes | No | Yes | Partial Yes | No |
| Cost (10 yr. Capital outlay) | \$40M – \$80M | \$10M – \$20M | \$50M – \$100M | \$35M - \$70M | \$10-\$15M |
|  Benefits | <ul style="list-style-type: none"> Central source of cleansed, standardized and consolidated master data Minimal footprint and impact to existing architecture Provides the ability to define group and user level rights Creates golden record at both department and state levels | <ul style="list-style-type: none"> Can track the activities of data users to understand data usage, the most important data sets/records, related datasets, and the nature of those relationships. Advanced insight will include data lineage and historical information as data records evolve over time among agencies | <ul style="list-style-type: none"> Benefits of option 1 and 2 apply here | <ul style="list-style-type: none"> IDXR is used to create a common Citizen ID across different systems / applications. Can track the activities of data users to understand data usage, the most important data sets/records, related datasets, and the nature of those relationships. | <ul style="list-style-type: none"> IDXR is used to create a common Citizen ID across different systems / applications. |
|  Drawbacks | <ul style="list-style-type: none"> This approach does not update the original source record for those consolidated data elements. Does not provide insights into the PII metadata e.g., data usage, data access etc. | <ul style="list-style-type: none"> Only monitors the passive or active attributes of the datasets rather than the actual record No golden PII customer record is created | <ul style="list-style-type: none"> This approach does not update the original source record for those consolidated PII data elements. | <ul style="list-style-type: none"> IDXR functions like a registry MDM solution. This does not create a golden record. Unless expanded to and consolidated among all agencies, multiple instances of IDXr will be needed to a specific agency data regulatory or policy restrictions. | <ul style="list-style-type: none"> IDXR is used to create a common citizen id across different systems / applications. Can track the activities of data users to understand data usage, the most important data sets/records, related datasets, and the nature of those relationships. |

Evaluation Criteria: Total Value

37 of 191

| Assessment Area | Value Domain | Option 1: MDM | Option 2: Metadata Management | Option 3: MDM & Metadata Management | Option 4: IDXR & Metadata Management | Option 5: PII Process Management |
|--|----------------|---|---|---|---|---|
| Customer Centric / Self-Service | Business |  |  |  |  | NA |
| Future Needs and Functional Agility | Business |  |  |  |  | NA |
| Operational Efficiency | Business |  |  |  |  |  |
| Reporting and Analytics | Business |  |  |  |  | NA |
| Architectural Complexity | Technology |  |  |  |  | NA |
| Security, Data and Privacy | Technology |  |  |  |  |  |
| Resiliency | Technology |  |  |  |  | NA |
| Alignment to Market Trends | Technology |  |  |  |  | NA |
| Vendor Management Complexity | Execution Risk |  |  |  |  | NA |
| Time to Implement (Phased Approach) | Execution Risk |  |  |  |  |  |
| Change Management | Execution Risk |  |  |  |  |  |
| Cost of Ownership (High Level 10-year TCO) | Cost | \$40M – \$80M | \$10M – \$20M | \$50M – \$100M | \$35M - \$70M | \$10M-\$15M |



High Level Costs – Rough Order of Magnitude (ROM) 10-year Capital Cost*

| Cost Buckets | Option 1: MDM | Option 2: Metadata Management | Option 3: MDM & Metadata Management | Option 4: Entity Resolution & Metadata Management | Cost Buckets | Option 5: PII Process Management |
|--|---------------|-------------------------------|-------------------------------------|---|--|----------------------------------|
| Software Licensing (Cost for 10 yrs.) | \$20M – \$40M | \$5M – \$10M | \$25M – \$50M | \$15M - \$30M | PII Policy and Management Framework | \$500K-\$1M |
| One Time Implementation (1-3 yrs.) | \$10M – \$20M | \$2.5M – \$5M | \$12.5M – \$25M | \$10M - \$20M | PII Security Assessment Tooling and Knowledge Transfer | \$500K-\$1M |
| Ongoing M&O (7-9 yrs.) | \$10M – \$20M | \$2.5M – \$5M | \$12.5M – \$25M | \$10M - \$20M | PII Process Security Assessments | \$8M-\$13M |
| Total (10-year TCO) | \$40M – \$80M | \$10M – \$20M | \$50M – \$100M | \$35M - \$70M | Total | \$10M – \$14M |

*Note – this cost model shows an initial estimate of the 10-year capital cost of acquiring the technology or implementing the process. This initial estimate **does not include agency or OIT staff time or backfill / hiring requirements.**

Option 1: Master Data Management – PII Data

39 of 191

Master Data Management is a technology-enabled discipline in which business and IT work together to ensure the uniformity, accuracy, stewardship, semantic consistency and accountability.

| Description | Colorado Impact | Implementation Style | Security Considerations |
|--|---|--|--|
| <p>1. MDM is about maintaining a "single trusted version" for critical concepts that describe what an organization does. It would enabled the Departments and CO-OIT to work together ensuring the accuracy, security, and stewardship of the PII data.</p> | <p>1. A MDM solution will allow the State to bridge across fragmented silos of PII customer/citizen data and create a trusted customer/citizen profile (golden record).</p> <p>2. A comprehensive PII master data management approach consists of processes such as data collection, accumulation, data cleansing, data comparison, consolidation, quality control and data distribution within departments and across departments to ensure consistency and control.</p> | <p>1. MDM Solutions are typically implemented within 4 distinct styles (Consolidated, Registry, Centralized, & Co-Existence)</p> <p>2. Of the four implementation styles, a consolidated approach would best suit CO-OIT's needs and addresses HB21-1111 requirements (i.e. location and access of the golden record).</p> | <p>1. A Consolidated Style would require CO-OIT unite all identified PII element into a singular infrastructure.</p> <p>2. CO-OIT in conjunction with each agency, each agency would be required to identify all security and regulatory restrictions for PII data across the public agency domains as it attempts to consolidate.</p> <p>3. OIT would remain responsible for the maintenance of the MDM solution and PII data contained while each agency would continue to maintain their systems which contain PII data.</p> |

MDM implementation styles can vary dependent upon the organizational needs and objectives of data usage



Consolidation

Consolidation is used primarily to support business intelligence (BI) or data warehousing initiatives as the master data resides only within the data warehouse.



Registry

Registry uses a simple database, called a registry, as a cross-reference table to reconcile identifiers (such as customer numbers) in the various operational systems across the enterprise.



Centralized

Centralized establishes a well-managed and governed central repository for master data, which will hold a set of “golden records” that are accessed in a read-only fashion by all the operational and analytical systems.



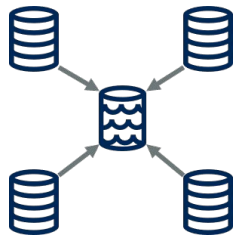
Coexistence

Coexistence is used in situations where the master data cannot be centralized and must be distributed in multiple locations throughout the enterprise. In other words, the coexistence style is used when multiple databases containing the master data must coexist.

Metadata Management is a set of capabilities that enables continuous access and processing of metadata that support ongoing analysis of information.

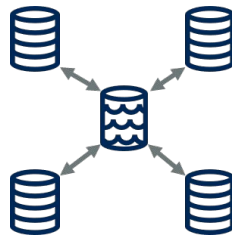
| Description | Colorado Impact | Implementation Style | Security Considerations |
|---|---|--|---|
| <ol style="list-style-type: none">1. Metadata Management Solutions serve to collate and communicate the inventory of data assets, communicate the business contexts of information, communicate the glossary of business terms, provide monitoring, auditing and traceability, and serve as a dynamic collaboration environment.2. Metadata Management Solutions will provide insight into data element Semantics, Location, Access, Trust, and Utilization. | <ol style="list-style-type: none">1. Metadata Solutions can provide a glimpse into the workflow of data, data consumption, and other attributes of identified datasets, | <ol style="list-style-type: none">1. MDM Solutions are typically implemented within three distinct styles (Centralized, Federated, & Distributed).2. Of the three implementation styles, a federated approach would best suit State's needs and addresses HB21-1111 requirements. | <ol style="list-style-type: none">1. While there are no critical elements contained within a metadata management solution, the behavioral data around utilization of critical data needs to be protected. Varying levels of security and regulation apply to active metadata capture by a metadata management solution. |

Metadata Management Solutions can be deployed in 3 potential styles



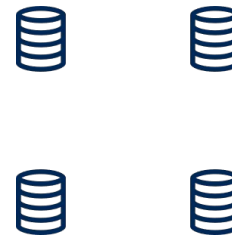
Centralized Architecture

- Metadata exists in a single database that stores nothing but metadata
- Contains a copy of metadata from other data sources
- Decision making is centralized, ensuring metadata is consistent across subsystems throughout the entire organization
- Data stewards and data users generally access a centralized metadata system via a single interface
- Requires integration with the source systems



Federated Architecture

- Each data system has a corresponding stand-alone metadata system within the constraints of a centralized technical framework and governance structure.
- Has ability to update real time metadata
- Decision making is also federated, centralized decision making on common PII i.e., GDAB ensuring metadata are consistent across subsystems throughout the entire organization
- Requires integration with the source systems



Distributed Architecture

- Each data system has a corresponding stand-alone metadata system.
- Metadata can be modified and updated without the need to coordinate with other systems
- Lack of integration between the systems
- Can lead to multiple terms for one item and, conversely, multiple items referenced by the same term.
- These "silos," autonomous and independent over time, and eventually unable to exchange data
- No integration with any system

Option 3: Master Data Management & Metadata Management

13 of 191

Combining Options 1 & 2 can enable Colorado to address each of the components of HB21-1111.

| Description | Colorado Impact | Implementation Style | Security Considerations |
|--|--|---|---|
| <ol style="list-style-type: none">1. The State would identify and implement Master and Metadata Management Solution(s) together. | <ol style="list-style-type: none">1. The combination of Master and Metadata Solutions will provide Colorado the necessary flexibility to create a map of where all PII elements exist while also moving towards a "golden record" for specific PII elements.2. Colorado would also garner the individual benefits of each of these dedicated deployments. | <ol style="list-style-type: none">1. Colorado could implement the same styles of Master and Metadata Solutions as suggested in Options 1 & 2.2. Colorado would be required to identify the connection points between these solutions to ensure full functionality is realized. | <ol style="list-style-type: none">1. While there are no critical elements contained within a metadata management solution, the behavioral data around utilization of critical data needs to be protected. Varying levels of security and regulation apply to active metadata capture by a metadata management solution.2. MDM and Metadata management solutions will maintain modern security functionality (i.e., encryption, authentication / authorization, etc.) |

Option 4: Entity Resolution & Metadata Management

44 of 191

Combining Option 2 with the existing IDXR solution can enable Colorado to partially address each of the components of HB21-1111.

| Description | Colorado Impact | Implementation Style | Security Considerations |
|---|--|---|--|
| <ol style="list-style-type: none">1. The State would identify and implement Metadata Management solution with the existing IDXR offering.2. IDXR currently resemble the "Registry" implementation style of a Master Data Management solution and provides an index and cross reference of PII data elements across linked systems. | <ol style="list-style-type: none">1. The combination of IDXR and Metadata Solutions will provide Colorado the necessary flexibility to create a map of where all PII elements exist. IDXR does not create a "golden record" but a registry of what PII assets relate to one another would be established.2. Colorado would also garner all the individual benefits of a Metadata Management Solution. | <ol style="list-style-type: none">1. Colorado could implement the same style Metadata Solutions as suggested in Option 2.2. Colorado would be required to identify the connection points between these solutions to ensure full functionality is realized. | <ol style="list-style-type: none">1. While there are no critical elements contained within a metadata management solution or IDXR, the behavioral data around utilization of critical data needs to be protected.2. Several deployments of IDXR could be established each with varying levels or security or regulatory needs which address agency-domain specific needs. |

Implementation Considerations

Required PII Controls Pre-Implementation Preparations

46 of 191

The following pre-implementation steps are necessary for ensuring that the State can implement one of these PII Data Management solutions. The below should be applied regardless of the solution chosen.



GOVERNANCE

Ensure that a single governance structure is established centrally for the project, with leads at the agency level and Colorado OIT. Currently, all Colorado agencies are federated with management of their PII and each agency owns their own data. Maintain the PII Advisory Board discussions to monitor project progress and discuss expansion.



CREATE A CONSISTENT DEFINITION OF PII ACROSS THE STATE

The Current State assessment identified that PII is still applied differently, with some agencies believing that an inclusion of one PII element makes a whole data set PII. Unify the view of items that do constitute PII from the GDAB definition of it (First and Last Name, SSN, etc.)



ADOPT THE GDAB DEFINITION OF PII TO DEPARTMENTAL POLICY

The Current State review identified that agencies are currently adapting the portions of the security policy that adheres to them. Apply a central security policy surrounding PII across agencies.



DATA & ANALYTICS STAFFING

Agencies have varying levels of data and analytics staffing and understanding. Enhance the maturity of the agencies by identifying a data steward either for the agency or by application for those with PII. Ensure the steward can speak to the quality of the data, ownership of it, how it's being used, etc.



PII TRAINING

Offer training to the agencies surrounding PII. Ensure they understand the definition, how to protect it, and who to notify if a question or issue occurs. Unify the application of the definition and protection of PII through training.



THIRD PARTY PII DATA OWNERSHIP

Ensure that a solution for security of PII data owned by third-parties is also considered as several agencies have this scenario. For data coming from third parties or being managed by third parties, governance is typically managed by Memorandums of Understanding (MOUs) or contract terms. Agencies have to take the data at their own risk. Ensure that each third-party application has the correct security parameters in place. From a list of 3rd party vendors, determine trust levels and how the data can be used.

Recommended PII Roles and Responsibilities

47 of 191

| Group or Role | Primary Focus | Responsibilities |
|------------------------------|---|---|
| Data Governance Leads | <ul style="list-style-type: none"> ▪ Chairs the Data Governance Committee ▪ Supports the CDO | The Data Governance Lead is responsible for enabling data governance at Departments through the DGC. The lead is accountable for management of the Data Stewardship organization, governance policy and standards setting. Accountable for a host of data definition and maintenance artifacts (e.g. data catalogues, dictionaries, metadata, MDM). |
| Data Owners | <ul style="list-style-type: none"> ▪ Own the business information ▪ Supports the Data Governance Committee | Data Owners are formally appointed business representatives within the Departments responsible for the defining the D&A policies and standards approved by the DGC. |
| Data Stewards | <ul style="list-style-type: none"> ▪ Monitor the business information ▪ Supports the Data Governance Committee | Data Stewards are formally appointed business representatives responsible for the implementation and enforcement of D&A policies and standards approved by the DGC. The Data Steward is responsible for monitoring data assets and usage against data standards and policies. When deviations from policy are detected, the steward is the key resource for issue resolution. Resident in key Lines of Business, they are the single data expert for the data in their Line of Business / Department. |
| Data Architect(s) | <ul style="list-style-type: none"> ▪ Data architects provide the technical leadership and direction needed for the D&A program ▪ Manage the data architecture needs for the D&A program | Data Architect(s) provides technical leadership and strategic direction for the technologies, standards, processes and architectures for D&A across the enterprise. They lead the design, development, implementation and maintenance of D&A data systems and solutions. They develop logical and physical data models to support D&A needs. They create and maintain current and target state data architectures. They support the process to define and manage standards, guidelines and processes to ensure data quality. They ensure technology solutions are in alignment with data architecture principles and target state. They oversee end-to-end data life cycle management activities. They work with IT teams, business analysts and D&A teams to understand data consumers' needs and develop solutions. They evaluate and recommend emerging technologies for data management, storage and analytics. |

Recommended PII Roles and Responsibilities

| Group or Role | Primary Focus | Description |
|---------------------------------------|--|--|
| Solution Architect(s) | <ul style="list-style-type: none"> ▪ Propose architecture solutions based on business and technology considerations. ▪ Create architectural designs to guide and contextualize solution development. ▪ Act as a bridge between technical and business audiences during solution development. | <p>A solution(s) architect is a technical leader with a deep understanding of business goals, business processes and solutions architecture who designs and supports the development of technology solutions to ensure that solutions meet business needs and align with architectural standards. Lead evaluation, design, and analysis of enterprise-wide solutions. Translates business and technical requirements into an architectural blueprint to achieve business objectives. Proposes solution recommendations and alternatives to satisfy customer needs. Collaborates with enterprise architecture, information security, applications and infrastructure teams to produce optimal designs. Produces technical documentation of systems and architectures. Ensures compliance of solutions to architectural standards. A Solution Architect acts as a subject matter expert on technologies and trends in your domain of expertise and as a consultant on a broad range of technologies, platforms and vendor offerings.</p> |
| Program Management Office | <ul style="list-style-type: none"> ▪ Led by designated PMO Leader ▪ Includes participation of Project Managers ▪ Supported by the CTO | <p>The PMO manages the delivery IT projects, working to ensure projects are executed on time, on budget and in scope. The scope of initiatives may broaden from IT-intensive projects to enterprise-wide business and IT initiatives.</p> |
| Change Management Lead/Analyst | <ul style="list-style-type: none"> ▪ Led by designated IT resource dedicated to IT Change Management | <p>The IT Change Manager is responsible for the overall quality of the Change Management process for IT implementations. This role is the key coordinator within the change process and is the core point of contact regarding changes for both the customer and the IT organization.</p> |
| Data Privacy Officer | <p>The Privacy officer will act as a point of contact between the the Department, CISO office and OIT.</p> | <p>This role is at the department level, the Privacy officer will be conducting regular assessments and audits to ensure privacy compliance and will maintain records of all data processing activities, as well as tracking the lifecycle of personal data within department and risks associated with processing it. The focus of this role is risk mitigation and the determination of the potential impact that loss of data would have on the business.</p> |

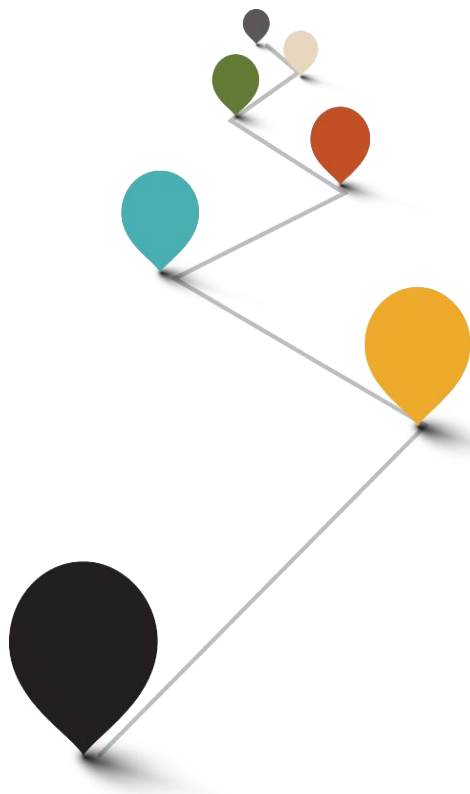
Recommended PII Roles and Responsibilities

49 of 191

| Group or Role | Primary Focus | Description |
|-----------------------|--|--|
| Data Security Manager | <ul style="list-style-type: none">▪ Facilitates a data security governance organization to help align setting of data security policy, enforcement of policy and execution of policy▪ Creates a risk-based process for the assessment and mitigation of any data security risk in an ecosystem consisting of supply chain partners, vendors, consumers and any other third parties▪ Conducts regular data security risk assessments to ensure that the organization's data security policies are being adhered to | <p>The data security manager (DSM) is responsible for establishing and implementing the data security governance framework to ensure that data assets and associated data processing activities are adequately protected in the digital ecosystem in which State of Colorado operates and compliant with regulatory requirements. This typically will involve identifying, evaluating and reporting on regulatory and security risk to data processing activities, while supporting and advancing business objectives.</p> <p>The DSM collaborates with the chief information security officer (CISO), data privacy officer (DPO), and chief data and analytics officer (CDAO) to create policies and controls for the appropriate protection of business data. A key element of the DSM's role is working with business leaders to determine acceptable levels of protection for the business data, and to implement practices that meet agreed policies and standards for data security.</p> |

Next Steps

50 of 191



- | | |
|----|--|
| 1. | Confirm Legislative need and direction from the JTC given the five PII Data Management solution Options, i.e. remove Options if possible given legislative direction |
| 2. | Develop business cases for a PII Data Management Solution, identifying needs at each agency, confirm scope (including whether non OIT-supported agencies opt in) |
| 3. | Complete a benefits analysis for PII Data Management project |
| 4. | Discuss potential high-level implementation plans for the remaining options |
| 5. | Develop a Total Cost of Ownership model for the top two implementation plans / options |
| 6. | Identify top use cases that can serve as pilots, implement on an agency-by-agency basis |
| 7. | Develop the TCO Model into a project budget and business case and request legislative approval |

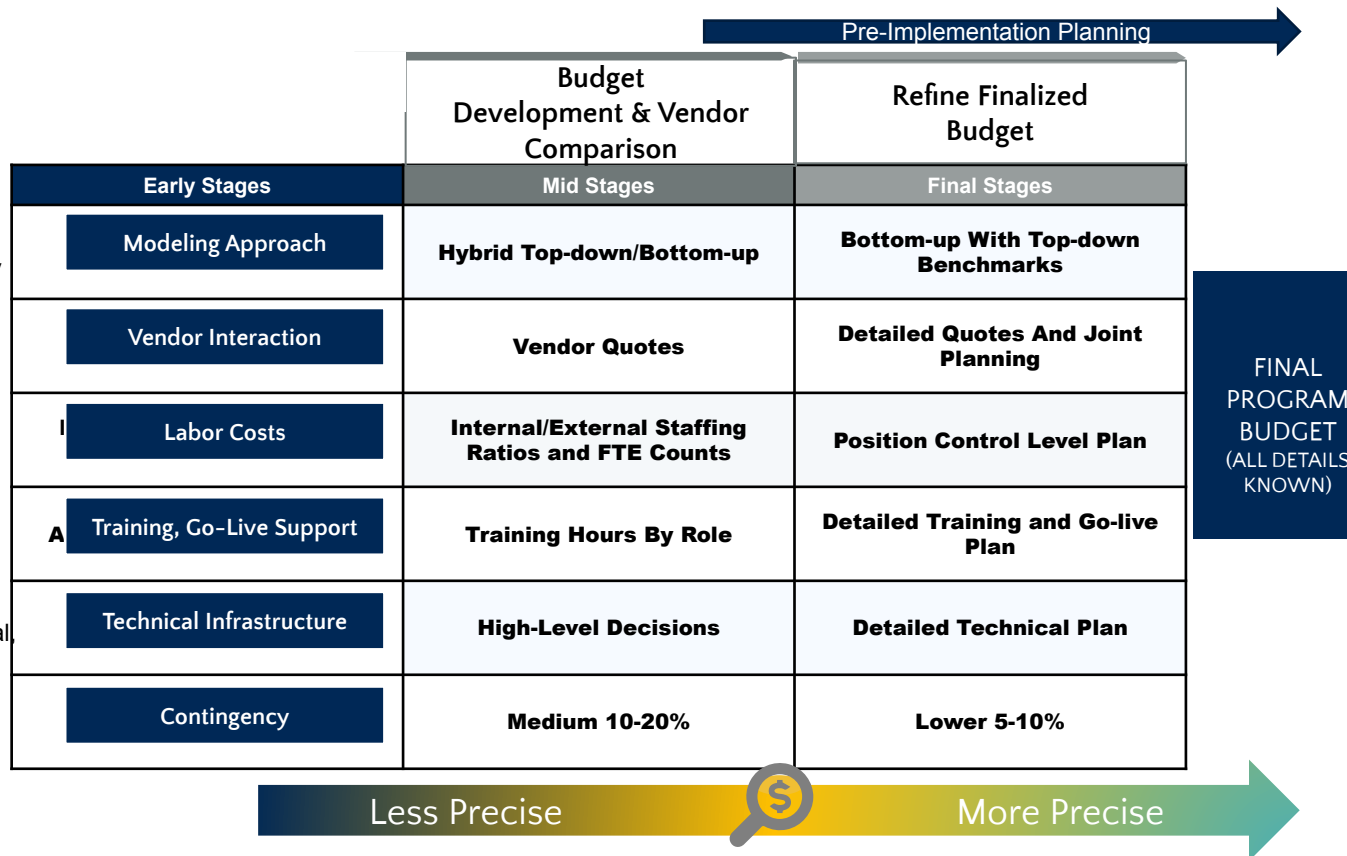
Typical Total Cost of Ownership Structure

51 of 191

TCO Models are usually created and then refined as the Procurement Process moves forward

Components:

- Cost projections for each option across primary cost components:
 - Licensing
 - Integration
 - Hardware and infrastructure
 - Labor and services
 - Training and Go-Live support
 - Extract production & data archiving
- Decommissioning savings
- One-time implementation costs (vendor, internal, contract)
- Ongoing maintenance expenses



Bharat Bagaria

Expert Partner
Gartner Consulting
Phone: +1 916 210 0907
Email: bharat.bagaria@gartner.com

Chelsea Wyatt

Senior Managing Partner
Gartner Consulting
Phone: +1 303 590 8599
Email: chelsea.wyatt@gartner.com

Farhat Naweed

Senior Director
Gartner Consulting
Phone: +1 475 685 5848
Email: farhat.naweed@gartner.com

Nikhil Nayak

Associate Director
Gartner Consulting
Phone: +1 916 213 7447
Email: nikhil.nayak@gartner.com

Lauren Talyor

Account Executive
Gartner
Phone: +1 205 837 3693
Email: lauren.talyor@gartner.com

Appendix: Overview

What Is Master Data?

54 of 191

- The least number of consistent and uniform set of identifiers and attributes that uniquely describe the core entities of the enterprise and are used across multiple business processes



| Master Data Examples | |
|--|--|
| <ul style="list-style-type: none"> Title First Name Family Name Date Of Birth Residential Address Email Phone Number(s) Government Assigned Identifiers (Driving License, National Identity, Passport) | <ul style="list-style-type: none"> Identifier(s) (SKU, GTIN, UDI) Weight Dimensions Color(s) Materials/Ingredients Country of Origin |
| Other Data Examples | |
| <ul style="list-style-type: none"> Transactions Social Media (Shares, Likes) Product Reviews Behavioural Interactions Segmentation | <ul style="list-style-type: none"> Price Inventory Lead Time Orders Sales/Profitability Returns |

Source: [Which Data Is Master Data?](#)

(G00120165) DISTRIBUTION

54 © 2021 Gartner, Inc. and/or its affiliates. All rights reserved.

MDM and Metadata Management

Solution Architecture Background



Master Data Management (MDM)

Master Data Management is a technology-enabled discipline in which business and IT work together to ensure the uniformity, accuracy, stewardship, semantic consistency and accountability

MDM is about maintaining a "single trusted version" for critical concepts that describe what an organization does. Instead of individual users, departments or business units using their own data and data sources.

Core MDM capabilities:

- Breaks down data silos
- Creates a single trusted view across the enterprise
- Assures process integrity for data creation
- Enables data sharing
- Offers a view into source data



Metadata Management

Metadata is any data that is used to enhance the usability, comprehension, utility or functionality of any other data point. It is commonly referred to as "data about data."

Without effective metadata management, the information infrastructure will provide suboptimal results, and there will be less ability to locate and leverage data.

Core metadata management capabilities:

- Offers metadata repositories
- Holds a business glossary
- Provides rule management and semantic frameworks
- Tracks data lineage
- Provides impact analysis
- Creates metadata ingestion and translation

Master Data Management (MDM)

- Introduction**
- Critical Components for MDM Programs**
- Security Considerations**

What comprises Master Data and how does this overlap with critical data elements?

- With a data-driven business environment comes an increased risk of data breaches, cyber attacks, phishing and more. This risk is increased with fragmented data that is distributed across many different systems and applications.
- A Master Data Management (MDM) solution will allow the State to bridge across fragmented silos of PII customer/citizen data and create a trusted customer/citizen profile (golden record) and ultimately deliver differentiated customer/citizen experiences.
- A comprehensive PII master data management approach consists of processes such as data collection, accumulation, data cleansing, data comparison, consolidation, quality control and data distribution within departments and across departments. This ensures PII consistency and control of use in various operational and analytical applications.

MDM Essentials Across People, Process and Technology

- Trusted master data is required in order to become a data-driven organization and it is a foundational requirement of digital business and business agility.
- Master data management gives your business users accurate, reliable, complete, 360-degree view of your data that can be used for insights, analytics, and business intelligence.
- For a successful MDM implementation define and articulate the links between the MDM program and the business outcomes and engage with business leaders early.
- An MDM implementation gets you data that is fit for purpose, ready for use, and can be a reliable source of information for your teams.

MDM Essentials Across People, Process and Technology

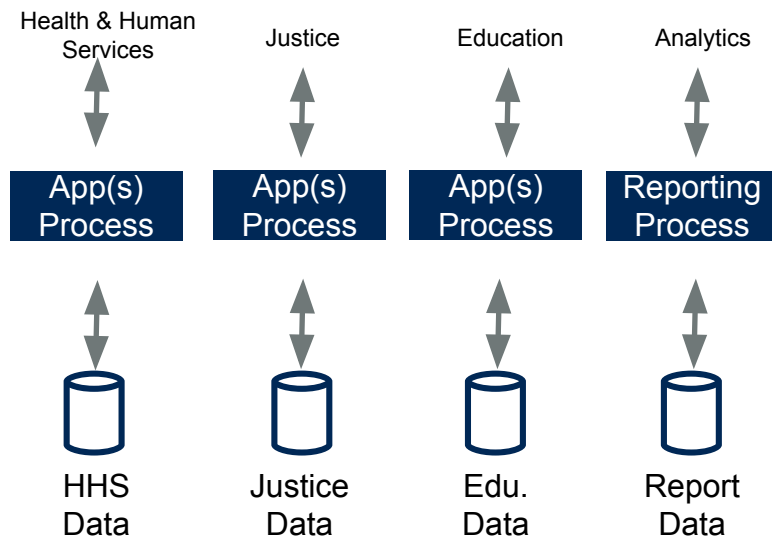


Source: Gartner
730039_C

MDM Value to the Organization

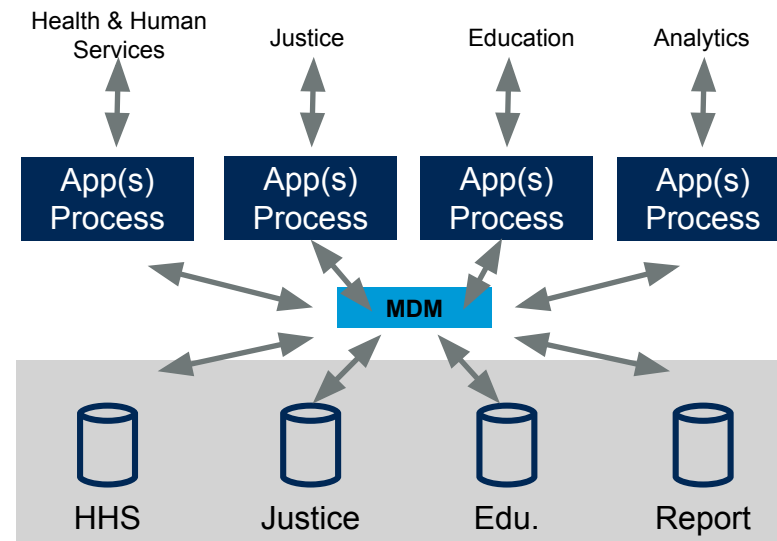
59 of 191

Before MDM



OR

After MDM

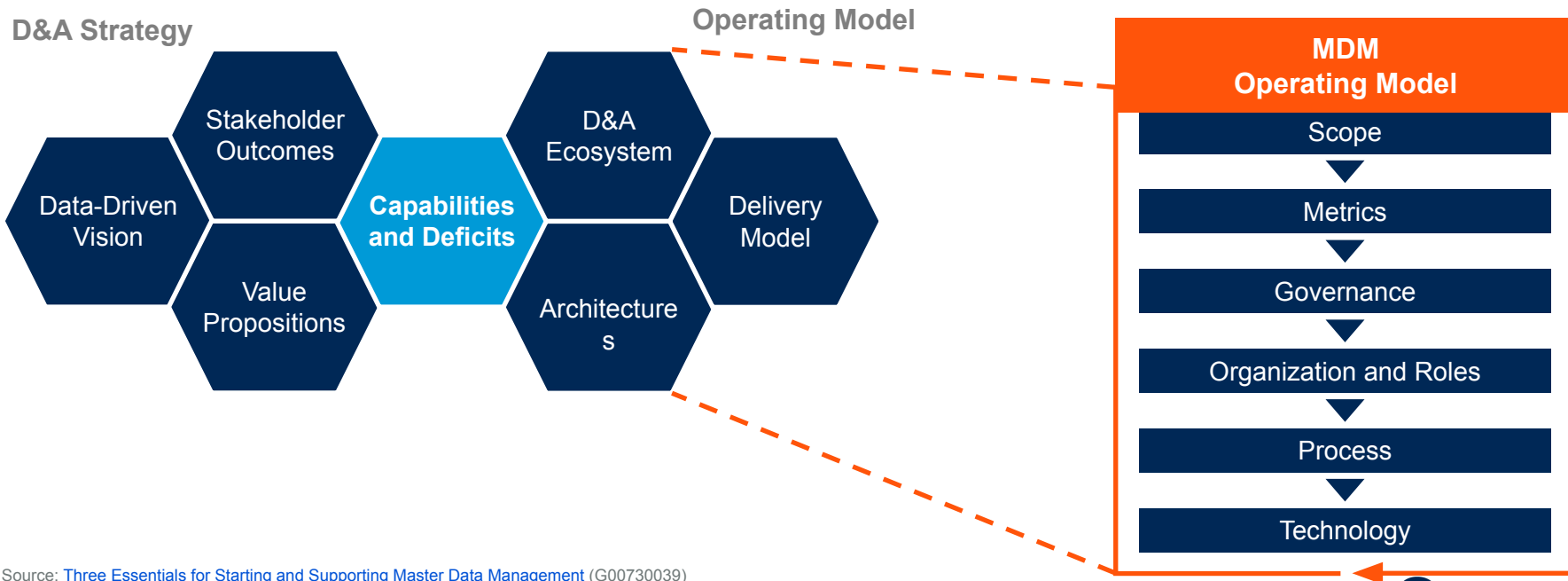


... One Curated Foundation

A Programmatic Approach to MDM

60 of 191

- The data management strategy and the operating model are intimately related.
- The operating model is informed by the strategy and as such, MDM, as part of the operating model should be in service of clear business outcomes.
- MDM operating model includes 6 components that have proven successful in organizing and focusing attention on the critical success factors for MDM programs



Source: [Three Essentials for Starting and Supporting Master Data Management](#) (G00730039)

RESTRICTED DISTRIBUTION

First: Scope - defines the boundaries of the MDM program

- Defines the boundaries of the MDM initiative.
- Adopt a think big, start small, deliver incremental business value approach.
- Requires business-level agreement on business outcomes and their priorities.
- Always link all MDM activity to business outcomes.
- Demands an ongoing collaborative effort among stakeholders.

| |
|----------------|
| 1. Scope |
| 2. Metrics |
| 3. Governance |
| 4. Org & Roles |
| 5. Process |
| 6. Technology |

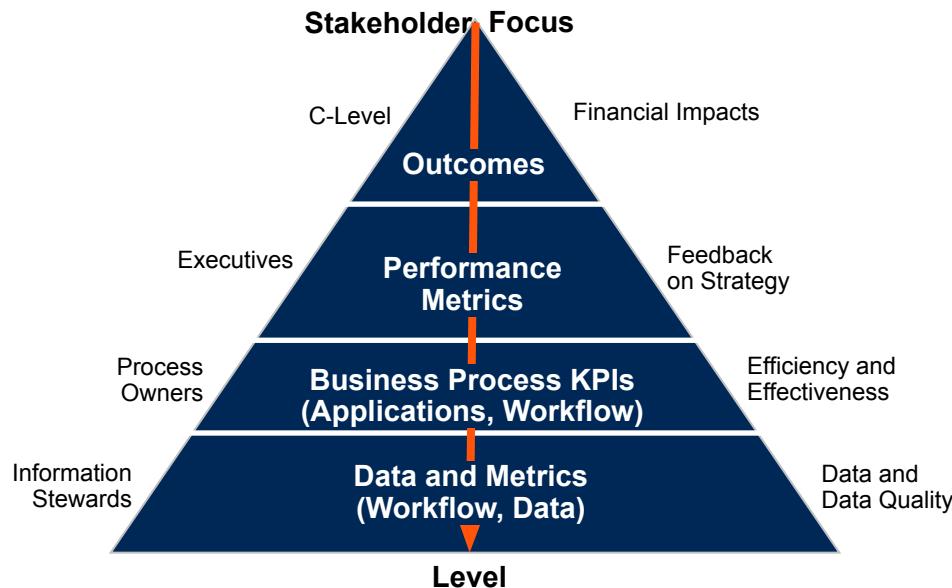


Source: [Articulating MDM Value to the Business](#) (G00732611)

Focus on the use cases that will have the biggest impact on the business and agree upon what will be delivered. Additionally, align all MDM activity with a prioritized set of business outcomes use cases.

Second: Metrics – these are key to linking MDM to value creation

| |
|----------------|
| 1. Scope |
| 2. Metrics |
| 3. Governance |
| 4. Org & Roles |
| 5. Process |
| 6. Technology |



Enterprise: Increase revenue by 5% via customer service and leverage in referencing prospects *by FY end.*

Supply Management: Customer responsiveness* target: *Improve from current 93% to 98% by end of Q3.*

Order Fill Rate =

$$\frac{\text{Total number of orders filled correctly}}{\text{Total number of orders}}$$

Master Data: Customer, Products/Services

Application Data: Customer, Product/Service, Order Qty

Transaction Data: Date, Actual Qty Shipped, Product/Services, Warehouse

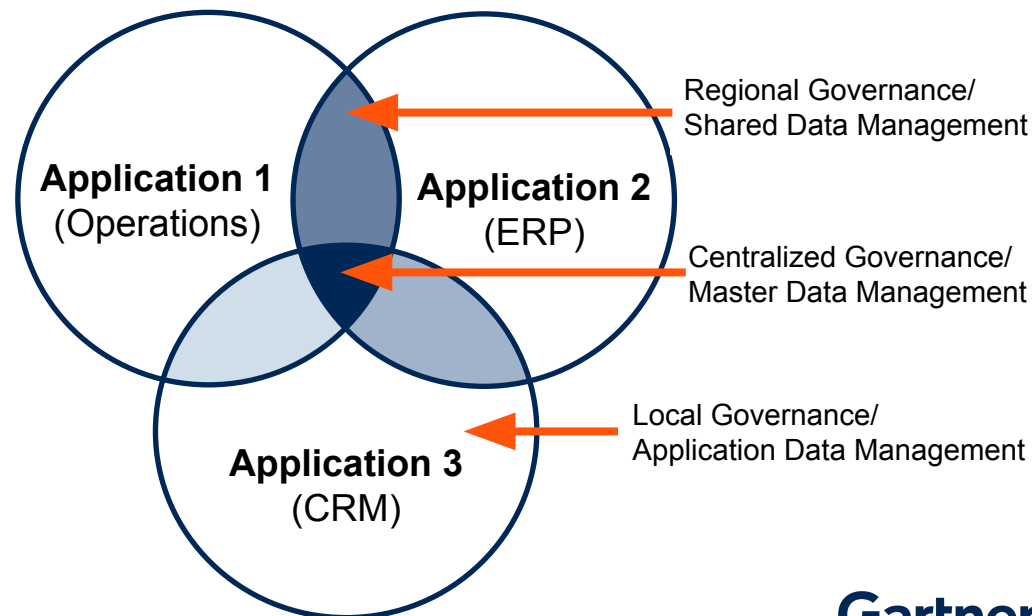
Source: [7 Steps to Build a Successful Business Case for MDM Programs](#) (G00719768);
 Tool: [How to Connect Data and Analytics to Business Value](#) (G00731241)

Directly connect MDM activity with business outcomes and priorities.

| |
|----------------|
| 1. Scope |
| 2. Metrics |
| 3. Governance |
| 4. Org & Roles |
| 5. Process |
| 6. Technology |

Third: Governance - Governance of designated master data is often the starting point for a broader information governance program spanning the enterprise

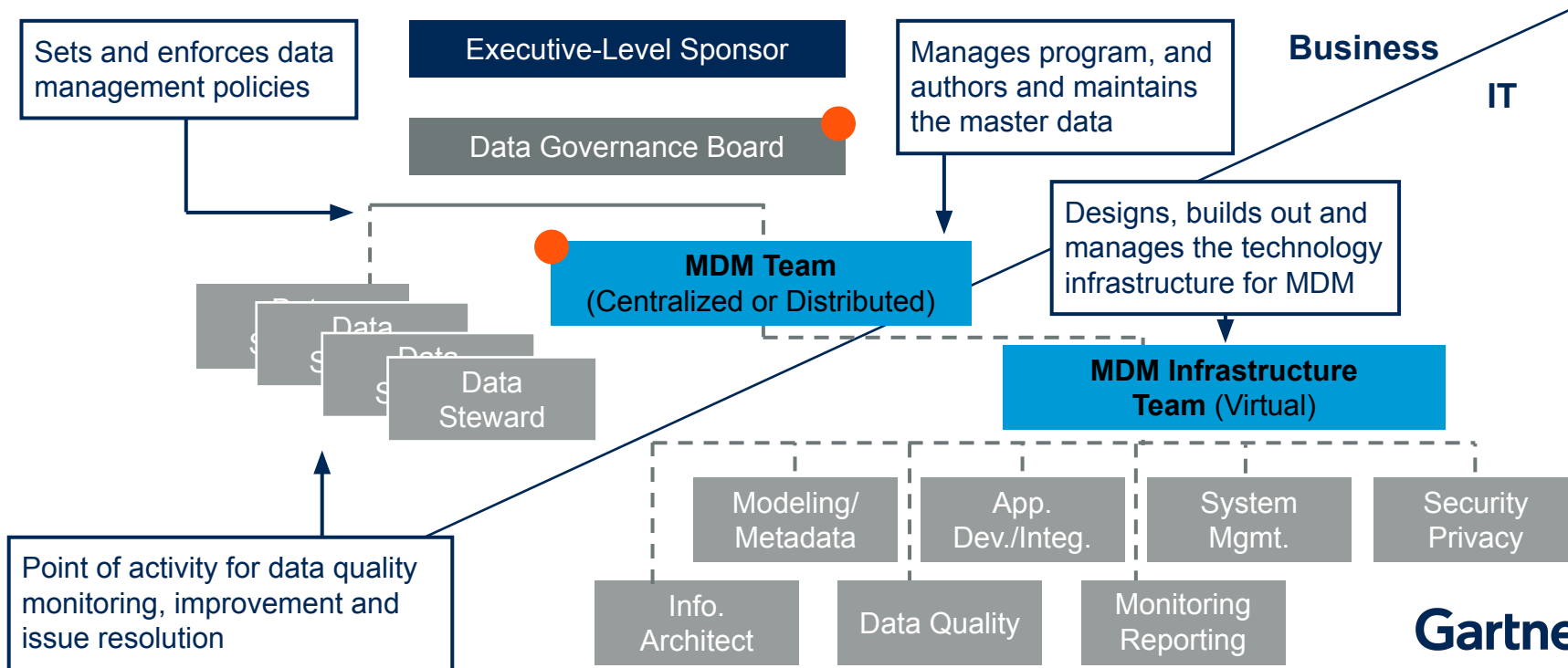
- **Governance:** The specification of **decision rights** and an **accountability framework** to ensure the **appropriate behavior** in the valuation, creation, consumption and control of data.
- Not all data is created equal.
- Master data is often the starting point for a broader information governance program.
- Defines a policy management framework to ensure master data quality throughout the business value chains.



| |
|----------------|
| 1. Scope |
| 2. Metrics |
| 3. Governance |
| 4. Org & Roles |
| 5. Process |
| 6. Technology |

Fourth: Organization & Roles - Governance or stewardship of master data will come more readily when the MDM initiative is clearly linked to outcomes business stakeholders care

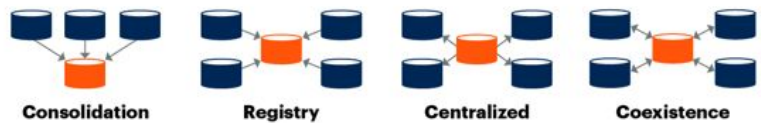
IT Representation



Fifth: MDM implementation styles can vary dependent upon the organizational needs and objectives of data usage

- There are four foundational implementation styles that are typically implemented successfully by organizations pursuing MDM.
- These implementation styles involve more than architectural patterns. They encompass the technical architecture, the system design, the scope of the MDM effort, and the invasiveness of the MDM effort, from both a business-process perspective and a technical-source-system perspective.
- A basic understanding of these implementation styles is required to determine the path best suited to the organization's maturity and ambition.
- The implementation styles are not mutually exclusive. For example, consolidation style might be used for customer data, and centralized style for product data. It is also not uncommon to start with one style and evolve to others.
- The implementation styles may also be used in combination. For example, placing a registry within a data warehouse for master data would, in essence, combine the consolidation and registry styles.

Four Foundational MDM Implementation Styles



| | Consolidation | Registry | Centralized | Coexistence |
|----------------------------|---|---|---|----------------------------------|
| Authorship vs. Hub | Author is separate from hub | Author is separate from hub | Authorship or harmonization takes place in hub | Author anywhere |
| Persistence vs. Hub | Hub stores copy separate from author/source | Hub stores index for master data; master exists at edge | Master persists in hub, though copies may exist at edge | Persist anywhere |
| Validation | Hub is system of reference | Hub is system of reference | Hub is system of record | Mixed system of record/reference |
| Primary Consumer | Downstream analytics and reporting | Both operational and analytical | Upstream operations | Upstream operations |
| Data Latency | Batch to real time | Batch to event-driven | Real time | Event-driven, publish-subscribe |
| Search Complexity | Relatively light | Very complex | Relatively light | Reasonably complex |

Source: Gartner
764706 C

Gartner will help determine the best-fit Customer PII MDM implementation style based on State of Colorado's specific business use cases; not biased towards any downstream implementation vendor/tool

66 of 191



Consolidation is used primarily to support business intelligence (BI) or data warehousing initiatives. The consolidation style need have no impact on operational systems — the cleaned up and well-managed master data resides only within the data warehouse.



Registry uses a simple database, called a registry, as a cross-reference table to reconcile identifiers (such as customer numbers) in the various operational systems across the enterprise. Think of the registry as a simple table in a relational database. It is important to note that, in the registry style, there is no golden record — merely a cross-reference table that links records that reside in the operational systems.

Gartner will help determine the best-fit Customer PII MDM implementation style based on State of Colorado's specific business use cases; not biased towards any downstream implementation vendor/tool



Centralized establishes a well-managed and governed central repository for master data, which will hold a set of “golden records” that are accessed in a read-only fashion by all the operational and analytical systems throughout the enterprise. The centralized style is applicable in situations where master data is authored, stored and accessed from a central system.

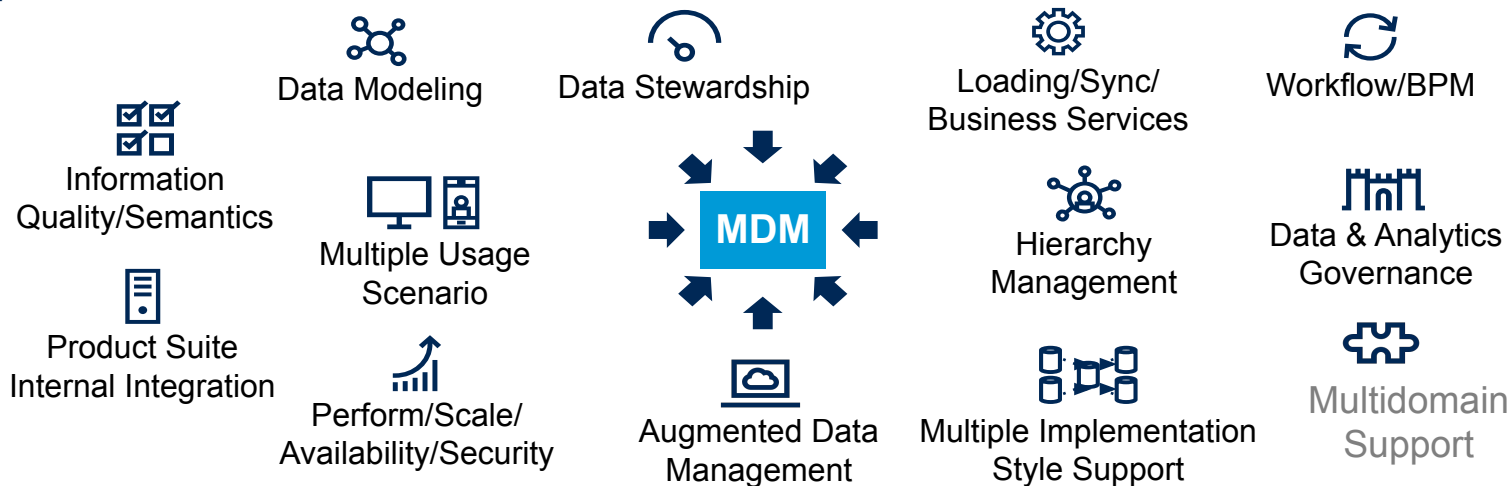


Coexistence is used in situations where the master data cannot be centralized and must be distributed in multiple locations throughout the enterprise. In other words, the coexistence style is used when multiple databases containing the master data must coexist. The coexistence style is the most complex of the MDM implementation styles because governance must be asserted in a distributed fashion over multiple databases, and complex data integration must be implemented to ensure that the data is kept consistent among the various databases.

Sixth: Technology

These Capabilities Work in Combination to Support MDM Business Requirements

| |
|----------------|
| 1. Scope |
| 2. Metrics |
| 3. Governance |
| 4. Org & Roles |
| 5. Process |
| 6. Technology |



Packaged MDM solutions are expected to address all of these requirements.

Benefits of Master Data Management

69 of 191

BUSINESS OPERATIONS & ACTIVITIES

- **Data Quality Management** : Master Data Management puts technical constraints on modifying a customer record, which prevents the creation of duplicate master data records.
- **Increased Usability and Efficiency**: Master Data Management allows for the widespread usability of specific data elements by reducing barriers and promoting data processing more efficiently and effectively.

IMPROVE DATA PROCESSES

- **Single Source of Truth**: Master data management provides a single source of truth to support business processes and decisions. With an efficient MDM process, end users can access updated, high-quality data to support operational and reporting / analytics processes.
- **Reduce Redundancy**: Eliminates data silos for same set of master data
- **Data Quality Management**: Master Data Management puts technical constraints on modifying a customer record, that prevents the creation of duplicate master data records.

ORGANIZATIONAL LEVEL BENEFITS

- **Remove/Reduce Slow Business Processes**: Master Data Management allows organizations to automate data processing which can prove time consuming.
- **Increase Agility**: MDM can provide improved agility for organizations. Access to reliable data will help with overcoming potential procedural challenges and allow organizations to continue to innovate.
- **Find Hidden Connections**: MDM can provide the ability to easily identify and visualize connections and many-to-many relationships across data categories and produce additional insight.

Data security governance framework used to mitigate business risks caused by security threats, data residency & privacy issues.

Creation of data security management framework, control catalogs and processes seamlessly integrated with data security and data governance could be strenuous but necessary to support business operations while implementing appropriate data security and privacy controls to mitigate business risks. The Gartner Data Security Governance (DSG) framework can be used in conjunction with other international and local standards to develop fit-for-purpose data security charters, control catalogs and processes

Relationship Between Data Security Management Frameworks, Control Catalogs and Processes



Addressing MDM Solution Security Concerns

71 of 191

There is an associated risk to PII data in an MDM system if appropriate data security controls are not put in place. To reduce this risk the State must develop an MDM strategy, which focuses on PII master data security for both PII data in motion and data at rest. The strategy should consider the following:

1

Leveraging application security provided by the MDM solution

Built-in solution security functionality can jumpstart the implementation of appropriate controls or restrictions for critical data elements

2

Assess, remediate and monitor sensitive data risks

Standardized policies for risk identification, management, and reporting will provide CO OIT increased insight into potential security incidents and ensure appropriate corrective actions are taken.

3

Collaborate with the State CISO to define data security policies

Garner input from security and data offices to ensure alignment with existing or upcoming policies or regulatory requirements.

Leveraging application security provided by the MDM solution

20191

User Authentication

MDM solution must have a user authentication management protocol in place to ensure the user or application has the right access to log into the MDM solution

User Authorization

MDM solution must provide the ability to create role-based user or application authorizations enabling access of data needed to complete the tasks allowed by the user or application

Record Audit

MDM solution must provide an audit trail and time stamp capabilities. This will provide the State with the capability to see who has requested or accessed which PII MDM records, when and where. This will trigger alerts and workflows to flag unauthorized behavior.

Assess, remediate and monitor sensitive data risks

73 of 191

PII data risk

Analyze and prioritize PII data risk. Leverage automated risk scoring to determine risk based upon specific security and privacy policies and relevant Federal and State Statutes. Monitor how PII data is used and by whom, as well as how data is moving within a department or across departments

Location of PII data

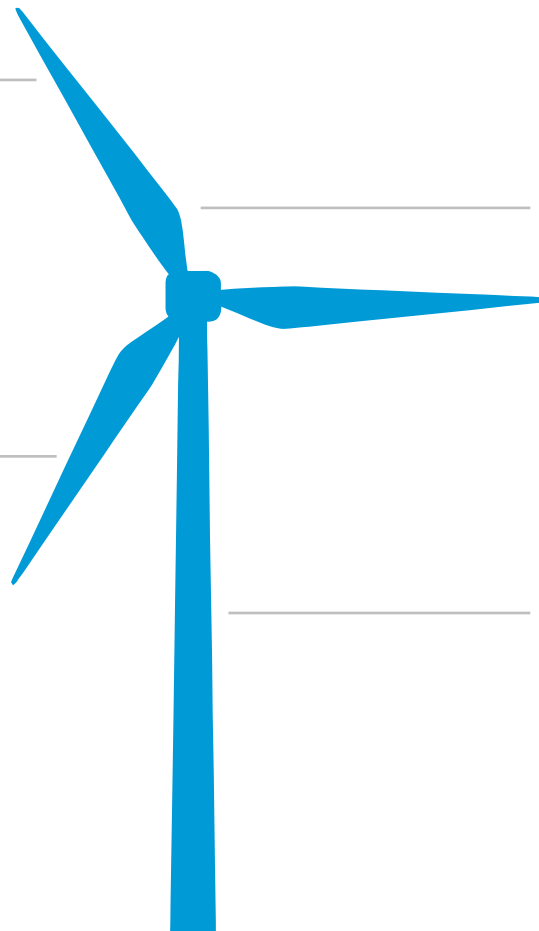
Understand where PII data assets reside in the source systems, MDM solution and other downstream systems

Data Security Protocols

Apply encryption, masking, tokenization and access controls to ensure only authorized users and applications have access to the data

Monitor data access

Monitor users for excessive or unusual access with user behavior analytics



Collaborate with the CISO to help define data and then implement data security policies and procedures

It is critical that data privacy policies are defined by the CISO with input from Data and Analytics leadership

01. Data Governance

- Guidelines, policies and standards to support data privacy and security
- Data cataloging
- Business Glossary
- Data Stewardship
- Data Lifecycle Management
- Data Usage / Data Sharing



02. Data Privacy

- Data Privacy Policies
- Federal and State Regulatory Requirements
- Federal and State Compliance Monitoring
- Data Classification

03. Data Security

- Data Access, Authorization, & Audit
- Data Security Tools and Resources
- Data Incident Reporting

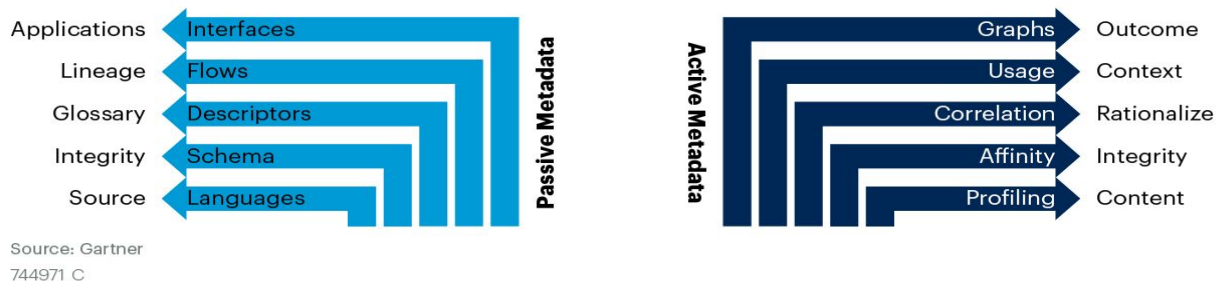
Metadata Management

- **Introduction**
- **Implementation Style**
- **Security Consideration**

Metadata management involves establishing policies and processes that ensure information can be integrated, accessed, shared, linked, analyzed and maintained to best effect across the organization.

76 of 191

Passive Metadata Versus Active Metadata



- **Passive metadata** is traditional design-based metadata such as data schema, but also runtime metadata that reports on how the design for integration, databases, file systems, data quality and many other operations execute their processing up to and including exception reporting.
- Passive metadata utilization employs lists, summaries, patterns and trends to **inform an external user or system without any expectation of action**, response or confirmation
- **Active metadata** is the continuous analysis of all available user, data management, systems/infrastructure and data governance experience reports to determine the alignment and exception cases between data as designed versus actual experience.
- Active metadata utilization includes the **capability of operationalizing** these analytic outputs in the form of operational alerts and generated recommendations. It identifies the nature and extent of patterns in data operations.

Foundational Capabilities That Leverage Metadata

77 of 191

Metadata repositories

Business glossary

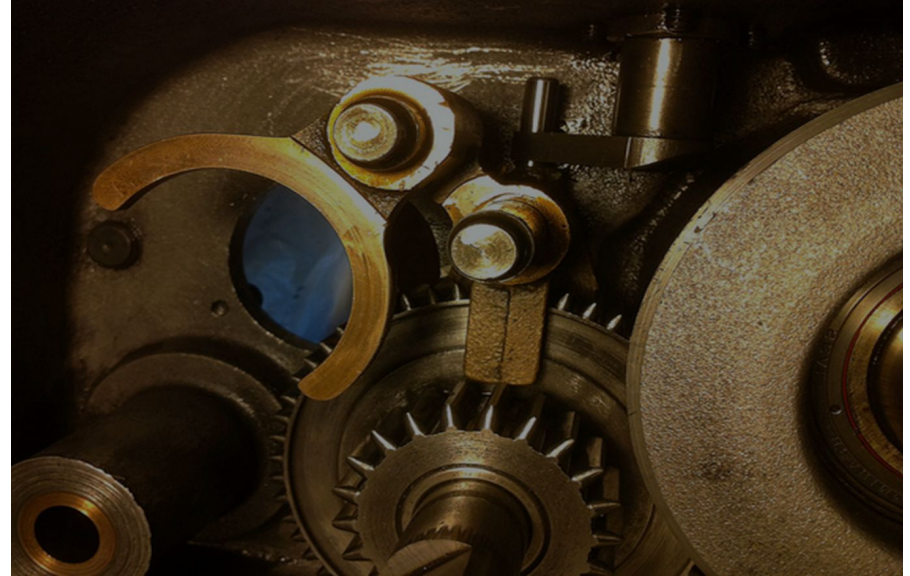
Data lineage

Impact analysis

Rule management

Semantic frameworks

Metadata ingestion and translation



Core Metadata Management Capabilities

Metadata repositories

Business glossary

Data lineage

Impact analysis

Rule management

Semantic frameworks

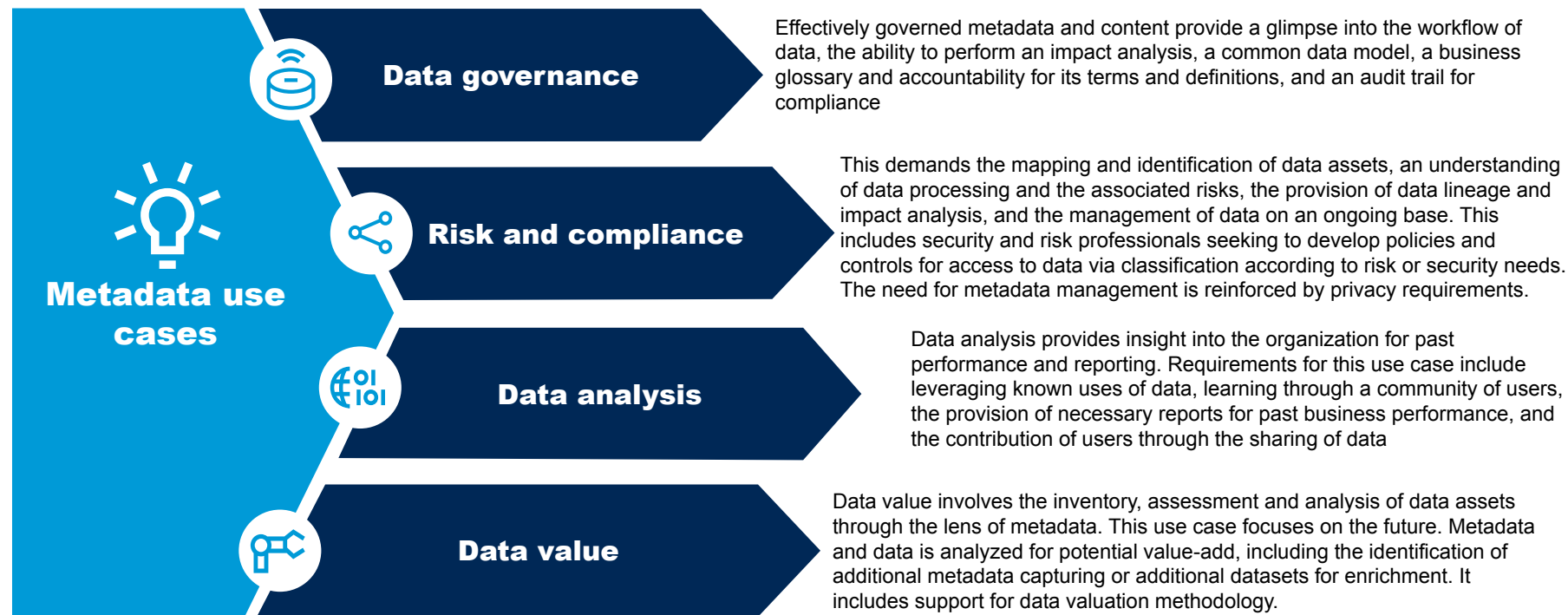
Metadata ingestion and translation



- **Collate and communicate the inventory of data assets** available to an organization, on an iterative and ongoing basis
- **Communicate the business contexts** (activities, processes, functions) within which those information assets are created, updated and consumed, for both operational and analytics cases
- **Communicate the glossary of business terms** that define the semantic interpretation and meaning of data, and provide mechanisms for mediating and resolving any definitional inconsistencies
- **Provide monitoring, auditing and traceability** functions to assist information governance processes
- **Serve as a dynamic collaboration environment** to enable business and technology colleagues to comment on, document and share data

Metadata management solutions need to support the critical requirements for data governance, risk and compliance, data analysis, and data value

9 of 191



Metadata can help provide insight into the value and associated risk of PII data

Through metadata, it's possible to identify what is happening within individual departments and across the departments. It can help prioritize value creation and manage risk associated with PII data.

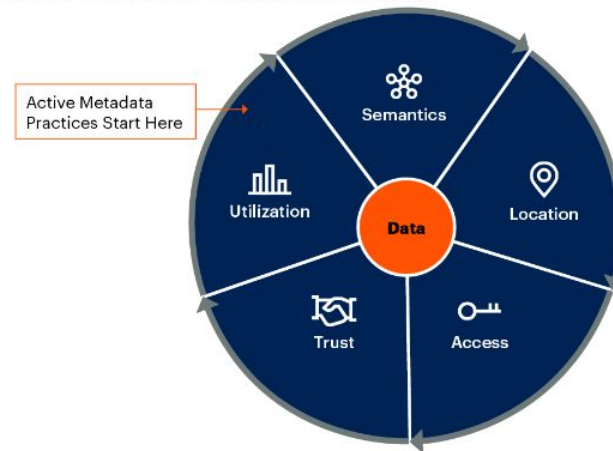
Metadata can help unlock the full potential of PII data and other data sets and help the business make better decisions.

Business users may discover new things about their data and solve business problems faster.

Gartner provides a metadata framework which is a collection of five metadata capabilities that describe data assets and can be used to unearth the hidden value of data:

- Semantics: Knowing what the data means in business terms
- Location: Mapping where the data resides and moves
- Access: Governing who has access to which data items
- Trust: Improving data understanding and trustworthiness
- Utilization: Studying data usage, popularity among user groups, relationships

Gartner's Metadata Capability Framework



Source: Gartner
758029_C

These capabilities provide unique insight into what is happening, and perhaps should not be happening within the enterprise

Data Semantics

- Inconsistent definitions for customer, order date or customer lifetime value, across marketing, sales and billing teams are a result of the lack of a common language. Semantics metadata can help you and your staff speak the same language.
- The word “semantics” refers to definitions / meanings. Data should be defined and managed at the level (or understanding) of common business users. For example, the data domain “party” could mean different things to different people. Breaking it down to usable forms like customer/prospect/supplier will make data consumption easier.

Data Location

- Location metadata can help unearth data flows that are not expected or even undesired (“undesired” as in the case of fraud). It can also help drive cost optimization efforts to inform better utilization of processing services.
- By analyzing location metadata, you can track where data has come from, who or what touches it, and where it goes. Sometimes this includes data outside your organization.

Data Access

- Enable self-service among your teams of business users. The fragmented data across systems and departments creates a challenge. Access metadata can inform what data one needs or restricted access to.
- Governance as a process remains central, but it doesn't have to be implemented or monitored that way.
- Classify data by information protection levels and label by domains. Study data usage patterns to inform policies around which data can go where and who can/should access it. Minimize data duplication. Avoid static data masking.

Data Trust

- Trust is a bigger issue than what metadata alone can solve. However, trust in your own data is a critical capability for becoming data-driven. Data trust focuses on the balance between data readiness and decision making.
- From running regular show-and-tell sessions to driving enterprise-wide data literacy programs, maximize business collaboration and education channels when addressing data issues related to semantics, location, access and trust.

Data Utilization

- Data consumption is a good measure of the impact that data creates in an organization. Utilization metadata gives an indication of the operational value realized from data. You can discover if your business processes and decisions are working well or missing the mark.
- Build capabilities to drive outcomes (such as data stewardship, data discovery and data privacy) from the insights created from metadata. Share data usage metrics with business users to drive further usability.

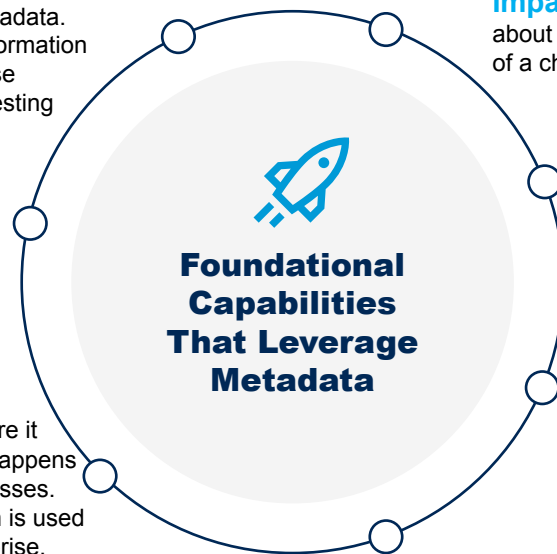
Foundational Capabilities That Leverage Metadata

82 of 191

Metadata repositories — Used to document and manage metadata, and to perform analysis using metadata. Organizations can also use repositories to publish information about reusable assets, which enables users to browse metadata during life cycle activities such as design, testing and release management.

Business glossary — A repository used to communicate and govern an enterprise's business terms, along with the associated definitions and the relationships between those terms.

Data lineage — Specifies data's origins and where it moves over time. Data lineage also describes what happens to data as it goes through diverse systems and processes. Data lineage can help with analyzing how information is used and tracking the flow of information across the enterprise, serving various purposes.



Impact analysis — Conveys extensive details about the dependencies of information or the impact of a change propagated from a data source.

Rule management — Automates the enforcement of business rules that are tied to data elements and associated metadata. This capability supports dedicated interfaces for the creation of, and the order of execution and links with, information stewardship for effective governance.

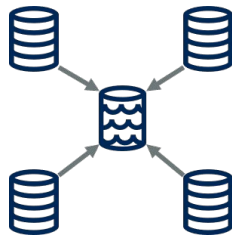
Semantic frameworks — Include support for taxonomies; entity relationship (ER) models; and ontology and modeling languages such as the Resource Description Framework (RDF), the Web Ontology Language (OWL) and the Unified Modeling Language (UML).

Metadata connectors for ingestion and translation

Using techniques or bridges for various data sources, such as:

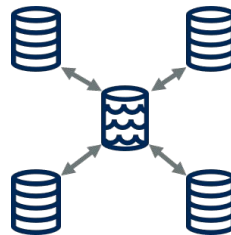
- Extraction, transformation and loading (ETL), application integration, data integration, search
- Business intelligence (BI) and reporting tools
- Business metadata
- System metadata administration and operations runtime metadata from networks, servers, communications nets, telemetry and other hardware specification and operations data

PII related Metadata can be captured in one of the 3 architecture patterns



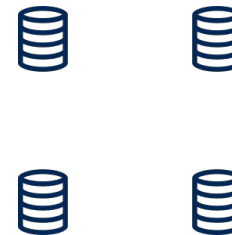
Centralized Architecture

- Metadata exists in a single database that stores nothing but metadata
- Contains a copy of metadata from other data sources
- Decision making is centralized, ensuring metadata is consistent across subsystems throughout the entire organization
- Data stewards and data users generally access a centralized metadata system via a single interface



Federated Architecture

- Each data system has a corresponding stand-alone metadata system within the constraints of a centralized technical framework and governance structure.
- Has ability to update real time metadata
- Decision making is also federated, centralized decision making on common PII i.e., GDAB ensuring metadata are consistent across subsystems throughout the entire organization.



Distributed Architecture

- Each data system has a corresponding stand-alone metadata system.
- Metadata can be modified and updated without the need to coordinate with other systems
- Lack of integration between the systems
- Can lead to multiple terms for one item and, conversely, multiple items referenced by the same term.
- These "silos," autonomous and independent over time, and eventually unable to exchange data

A Metadata management solution can help with securing your PII data

B.L.P.19



1 Identify the PII used by the departments.

Begin by identifying all the PII each department collects, processes and uses. Once identified, work with CISO to start planning your security and privacy strategy for protecting it.



2 Locate where PII is stored. PII data could be stored in any number of locations such as servers, on the cloud, excel spreadsheets etc. When locating data consider the following three data states: Data in-use, at-rest and in-motion. This will help you understand the various systems / applications that need to be protected



3 Classify PII in terms of sensitivity.

Once PII data has been located, classify it by the likelihood of being compromised and the possible consequences of the data being exposed. This helps with prioritization of which data and systems to protect first.



4 Establish a usage policy. For accessing PII.

This policy defines who can access PII and the acceptable way(s) to use it. This policy can serve as a jumping-off point for building technology-based controls to reinforce proper PII access and usage.



5 Implement an encryption solution.

Data-centric encryption will protect PII data from internal and external risks and put residents / citizens at ease when you ask for their most sensitive data.



6 Back up your solution with training.

Train employees frequently on any technology updates as well as evolving threats.

Target State and ROM

- **Option 1: Master Data Management**
- **Option 2: Metadata Management**
- **Option 3: MDM & Metadata Management**
- **Option 4: Entity Resolution & Metadata Management**
- **ROM of Cost for Options 1,2,3&4**

















Summary of Target State Options

86 of 191

| | Option 1: Master Data Management (MDM) | Option 2: Metadata Management | Option 3: MDM & Metadata Management | Option 4: Entity Resolution & Metadata Management |
|-----------|--|--|--|--|
| Approach | <ul style="list-style-type: none"> Implement Consolidation Style of MDM at the Department level As the organization matures consider implementation of consolidation style of MDM at the State level | <ul style="list-style-type: none"> Implement Federated Style of metadata management As the State mature as an enterprise, consider implementation of the metadata management solution at the enterprise level. This will accommodate the metadata associated with other data sets as well as PII | <ul style="list-style-type: none"> This is a combination of options 1 & 2 | <ul style="list-style-type: none"> Use existing IDXr architecture and expand based upon use-case classification or agency domain Implement federated style of metadata management |
| Benefits | <ul style="list-style-type: none"> Central source of cleansed, standardized and consolidated master data for downstream systems Minimal footprint and impact to existing architecture Provides the ability to define group and user level rights Creates golden record | <ul style="list-style-type: none"> Can track the activities of data users to understand data usage, the most important data sets/records, related datasets, and the nature of those relationships. Advanced insight will include data lineage and historical information as data records evolve over time among agencies | <ul style="list-style-type: none"> Benefits of option 1 and 2 apply here | <ul style="list-style-type: none"> IDXR is used to create a common citizen id across different systems / applications. Can track the activities of data users to understand data usage, the most important data sets/records, related datasets, and the nature of those relationships. |
| Drawbacks | <ul style="list-style-type: none"> This approach does not update the original source record for those consolidated data elements. Does not provide insights into the PII metadata e.g., data usage, data access etc. | <ul style="list-style-type: none"> Only monitors the passive or active attributes of the datasets rather than the actual record No golden PII customer record is created | <ul style="list-style-type: none"> This approach does not update the original source record for those consolidated PII data elements. | <ul style="list-style-type: none"> IDXR functions like a registry MDM solution. This does not create a golden record. Unless expanded to and consolidated among all agencies, multiple instances of IDXr will be necessary each addressing specific agency data regulatory or policy restrictions. |

Evaluation Criteria: Business Value

















87 of 191

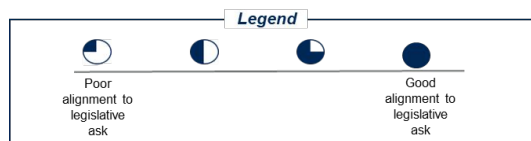
| Assessment Area | Criteria Description | Option 1: MDM | Option 2: Metadata Management | Option 3: MDM & Metadata Management | Option 4: Entity Resolution & Metadata Management |
|--|--|---|---|---|---|
| Business Value | | | | | |
| Customer Centric / Self-Service | Degree to which the solution functionality meets HB 21-1111 |  |  |  |  |
| Future Needs and Functional Agility | Level of flexibility of the solution to support evolving legislative requirements; configurability to support operational optimization (e.g., workflows, validations and other enhancements); time-to-production of changes and services |  |  |  |  |
| Operational Efficiency | Degree to which the solution addresses current functional and operational inefficiencies |  |  |  |  |
| Reporting and Analytics | Quality of standard and predictive analytics and the degree to which reporting tools available to business users enable operational performance analysis and improvements. |  |  |  |  |



Evaluation Criteria: Technology Value

















88 of 191

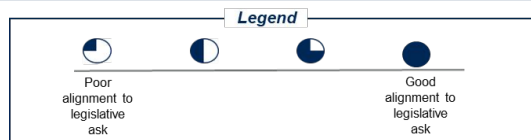
| Assessment Area | Criteria Description | Option 1: MDM | Option 2: Metadata Management | Option 3: MDM & Metadata Management | Option 4: Entity Resolution & Metadata Management |
|----------------------------|--|---|---|---|---|
| Technology Value | | | | | |
| Architectural Complexity | Complexity of technical architecture, integrations and data sources |  |  |  |  |
| Security, Data and Privacy | Ability of the solution to meet security, privacy and data protection needs |  |  |  |  |
| Resiliency | Ability of the solution to deliver enhanced operational stability and availability |  |  |  |  |
| Alignment to Market Trends | Alignment of the solution approach with broader direction of other states. <i>Where the market is going from a vendor perspective and a client perspective</i> |  |  |  |  |



Evaluation Criteria: Cost and Risk

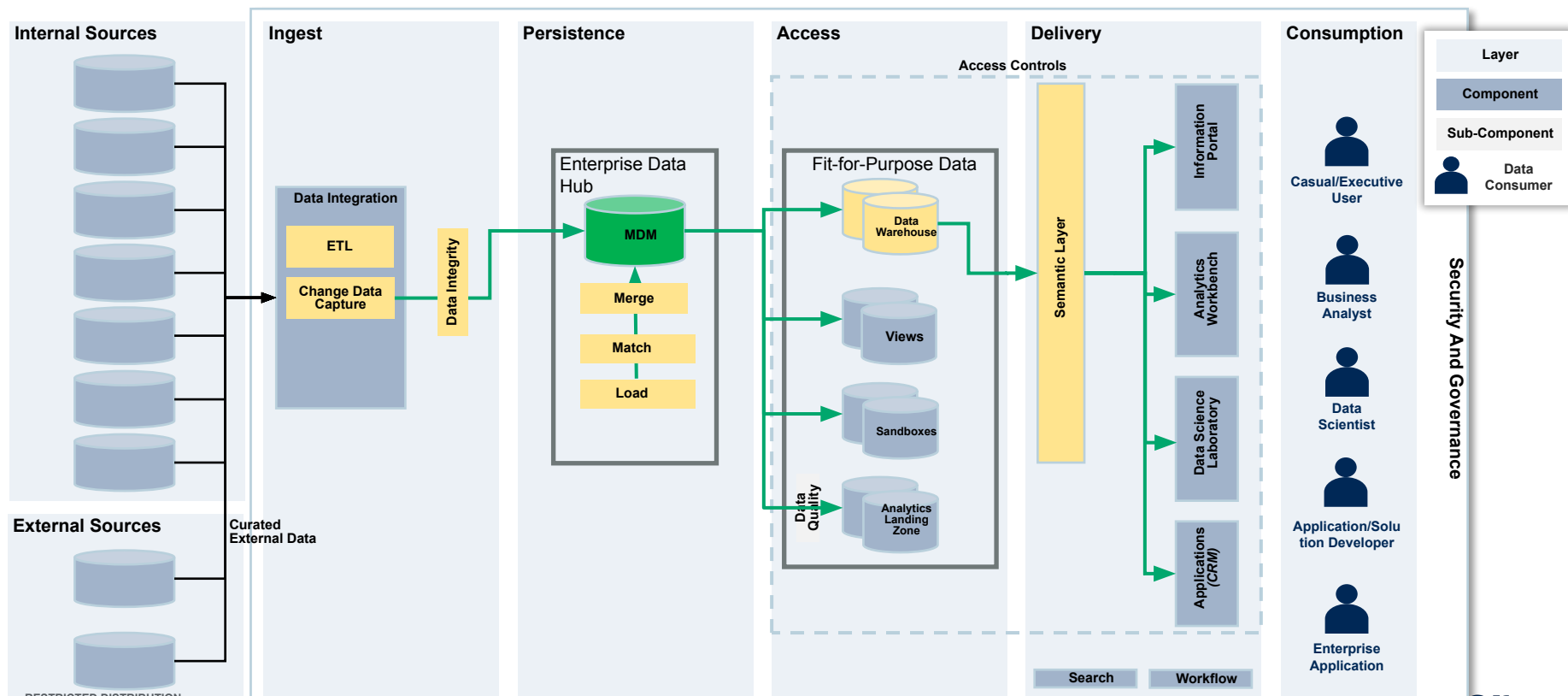
89 of 191

| Assessment Area | Criteria Description | Option 1: MDM | Option 2: Metadata Management | Option 3: MDM & Metadata Management | Option 4: Entity Resolution & Metadata Management |
|---|---|---|---|---|---|
| Execution Risk | | | | | |
| Vendor Management Complexity | The degree to which the solution option mitigates risks associated with coordination across multiple vendors, during both system implementation and subsequent operations |  |  |  |  |
| Time to Implement (Phased Approach) | The time it will take to procure, plan for and execute the implementation of all capabilities |  |  |  |  |
| Change Management | The degree of change and complexity of transitioning from current state to target state |  |  |  |  |
| Cost | | | | | |
| Cost of Ownership (High Level 10-year TCO) | Initial cost of implementation and on-going costs to maintain and support the solution |  |  |  |  |



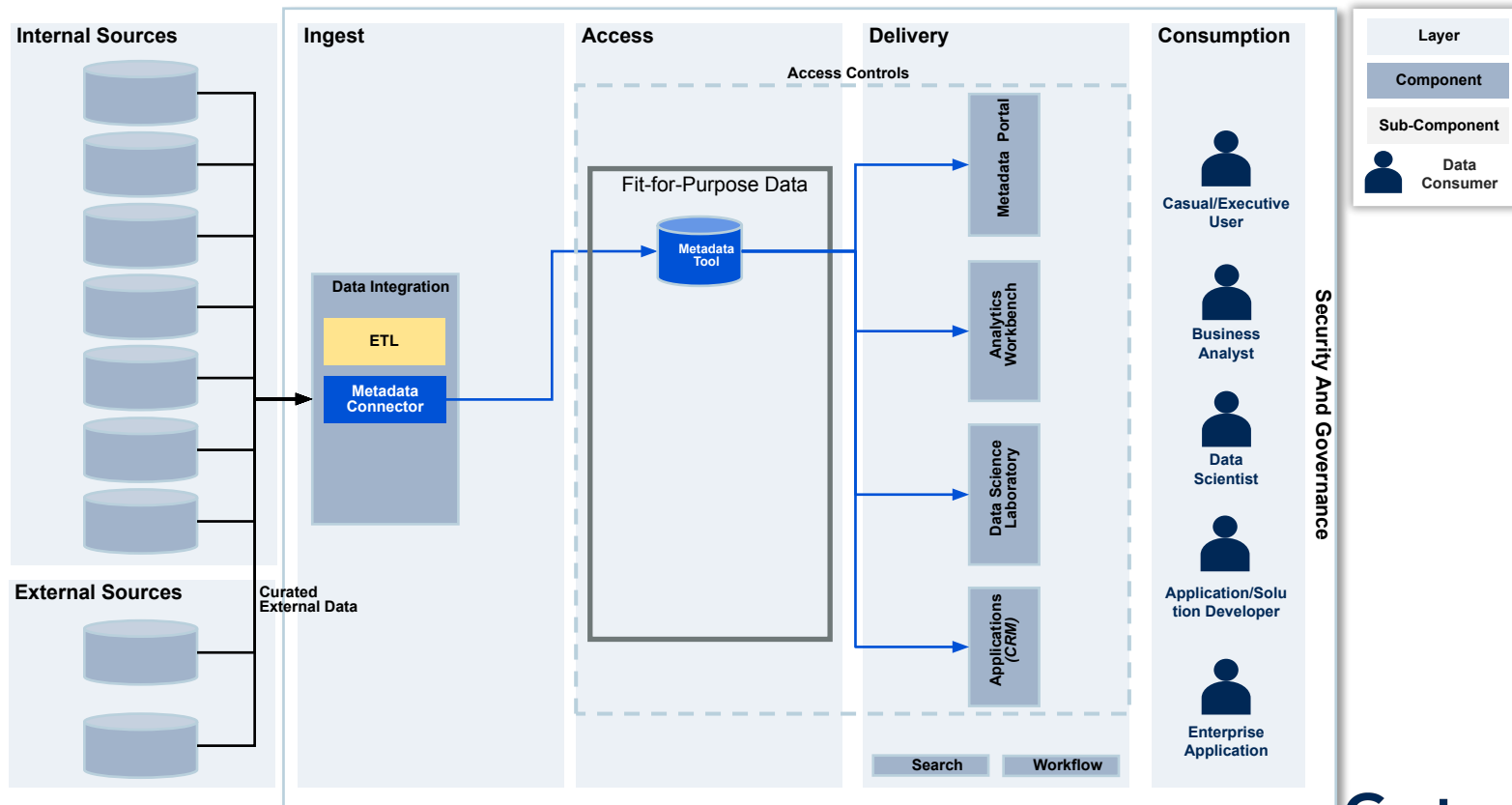
Option 1: Master Data Management – PII Data

90 of 191



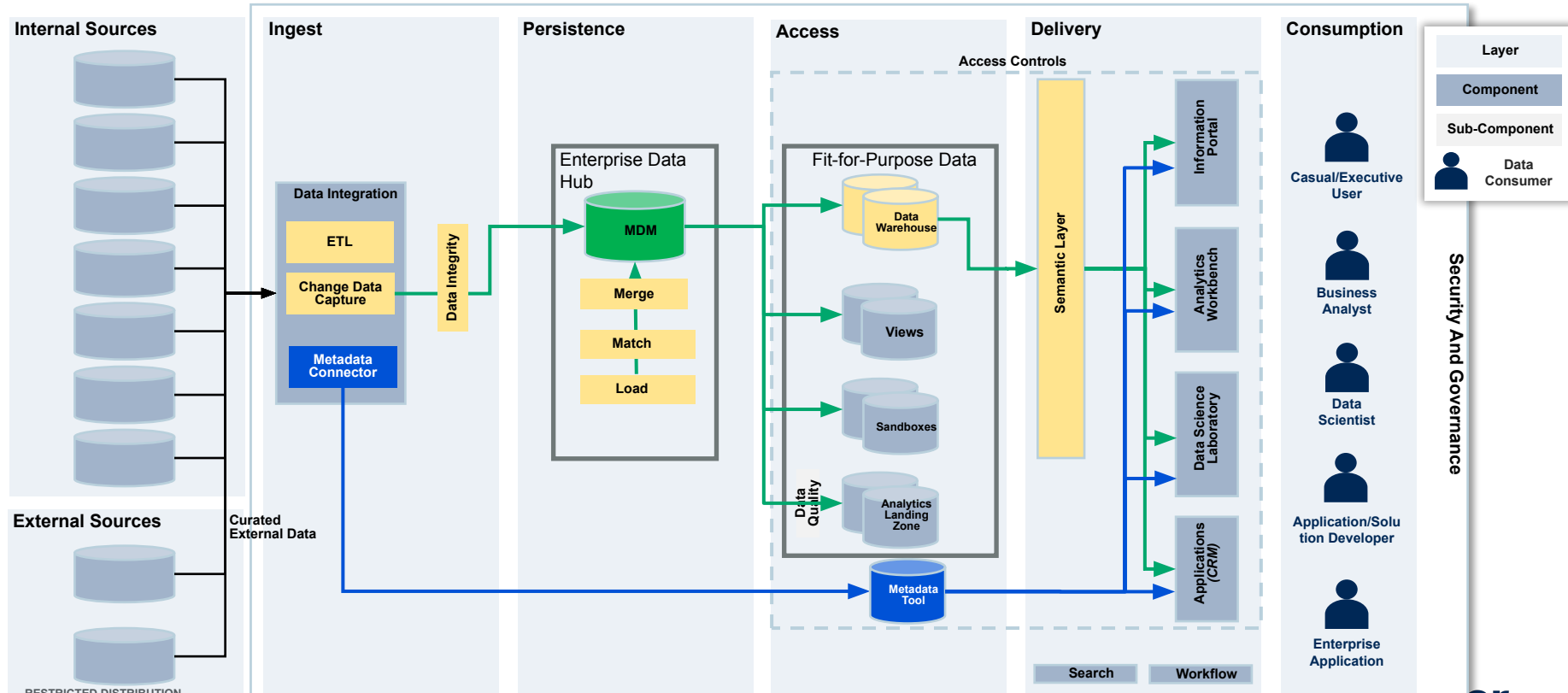
Option 2: Metadata Management Reference Architecture - Federated

91 of 191



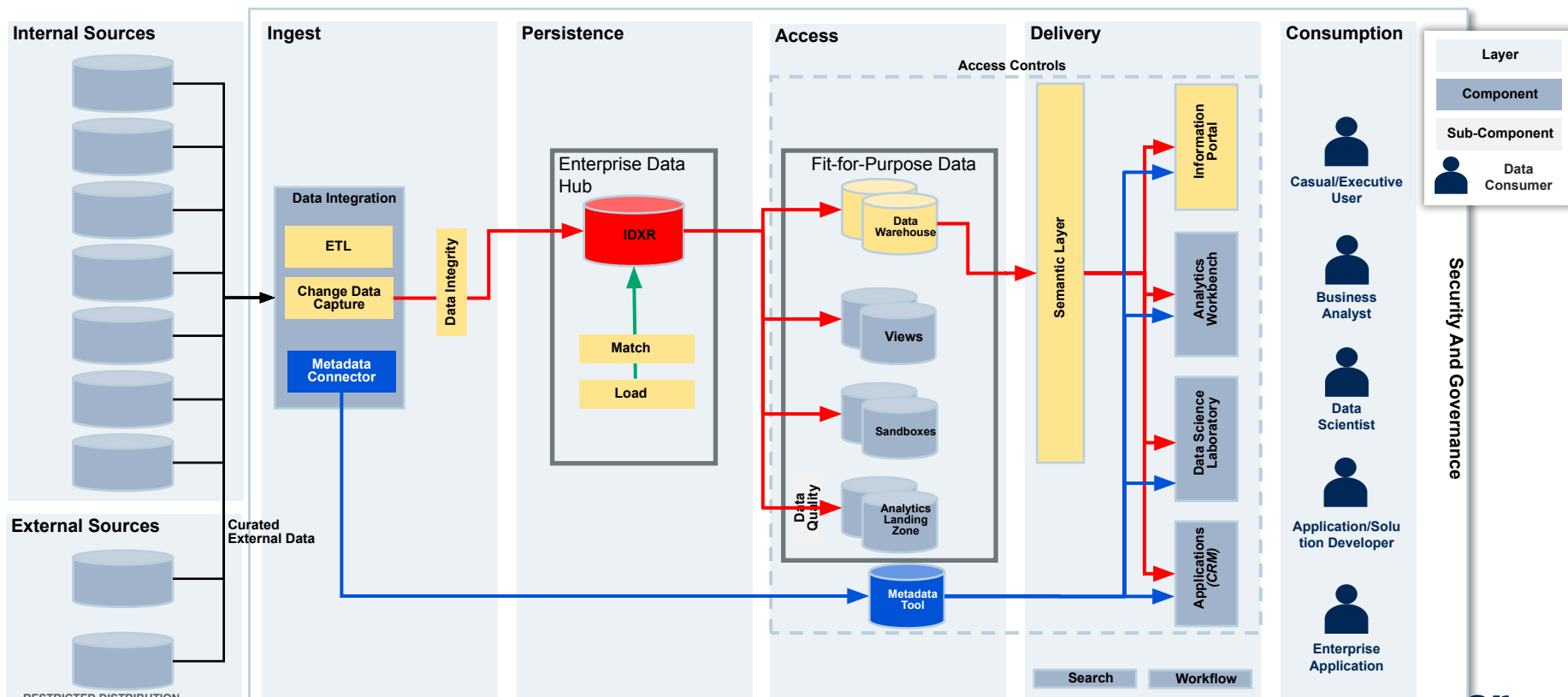
Option 3: Master Data Management & Metadata Management

92 of 191



Option 4: IDXR & Metadata Management

93 of 191



High Level Costs - ROM (10-year Total Technical Cost of Ownership)

94 of 191

| Cost Buckets | Option 1: MDM | Option 2: Metadata Management | Option 3: MDM & Metadata Management | Option 4: Entity Resolution & Metadata Management |
|---|---------------|-------------------------------|-------------------------------------|---|
| SaaS Licensing (10 yrs.) | \$20M – \$40M | \$5M – \$10M | \$25M – \$50M | \$15M - \$30M |
| One Time Implementation (1-3 yrs.) | \$10M – \$20M | \$2.5M – \$5M | \$12.5M – \$25M | \$10M - \$20M |
| Ongoing M&O (7-9 yrs.) | \$10M – \$20M | \$2.5M – \$5M | \$12.5M – \$25M | \$10M - \$20M |
| Total | \$40M – \$80M | \$10M – \$20M | \$50M – \$100M | \$35M - \$70M |

RESTRICTED DISTRIBUTION

Master Data Management Critical Capabilities

Magic Quadrant for Master Data Management

96 of 191

Demand arising from a variety of data and analytics initiatives drives strategic requirements for master data management solutions. This Magic Quadrant will help data and analytics leaders find the most appropriate vendor and solution for their organizational needs.

Quadrant Descriptions

Leaders

Leaders are frontrunners with offerings that support the full range of metadata management capabilities. They exhibit a clear understanding of, and vision for, where the market is headed, and are good at meeting customers' requirements for a variety of use cases.

Challengers

Challengers are well positioned in the light of key trends, but they may not provide the comprehensive breadth of functionality and support for use cases of the Leaders, or they may be limited to specific technical environments or application domains.

Visionaries

Visionaries demonstrate a strong understanding of emerging technology and business trends or have a position that is well aligned with current demand. However, they are not yet perceived as competitive players beyond their traditional customer base.

Niche Players

Niche Players have gaps in both their Completeness of Vision and Ability to Execute. They often exhibit a narrow focus in supporting particular use cases.

2021 Magic Quadrant



Critical Capabilities for Master Data Management Platforms^{97 of 191}

| Critical Capability | Definition |
|-------------------------------------|---|
| Workflow/BPM | The MDM solution should support a range of capabilities that include business process modeling, master data flow modeling and documentation, and analytics for key performance indicators and other benchmarking efforts in support of master data and MDM. |
| Loading/Sync/Business Services | The MDM solution should provide facilities for loading master data and integration middleware, including publish and subscribe mechanisms. It should also support, as necessary, the four MDM implementation styles, which each use loading, integration and synchronization in different ways. |
| Data Modeling | The MDM solution should effectively and flexibly support an organization's master data model requirements; model complex relationships between application sources inside an organization, and with intermediaries and other parties; and provide business-consumable metadata management capabilities. |
| Information Quality/Semantics | There must be facilities, in batch and real-time modes, for profiling, cleansing, matching, linking, identifying and semantically reconciling master data in different sources to create and maintain a "golden record." They may be provided directly or via tight integration with data quality partners. |
| Perform/Scale/Availability/Security | The MDM solution should meet demands for performance, scalability, availability and security, and have suitable availability characteristics. It should be able to manage privacy policies and rules, and to configure and manage different visibility rules in order to provide views for different roles. |

Critical Capabilities for Master Data Management Platforms (Cont.)

98 of 191

| Critical Capability | Definition |
|--------------------------|--|
| Hierarchy Management | The MDM solution should model and store multiple hierarchies within and across in-scope data domains to comprehensively classify all instances of master data for various business requirements, as well as for broad-based functions such as searching and reporting. |
| Data Stewardship | The MDM solution should support a range of capabilities, from information policy evaluation to day-to-day operation and management of MDM. It should support the role of business-led information steward. It should equip this role with a suitable UI through which services are provided. |
| Data Governance | The MDM solution should provide or support information governance functions — such as governance policy collaboration and creation, policy change management, and impact analysis — and react to changes made in an internal or external information governance layer. |
| Multiple Usage Scenarios | The MDM solution should support both operational and analytical MDM requirements, and any required integration between them — that is, both the operational and analytical usage of the data being mastered within the solution. |
| Multidomain Support | The MDM solution should have multiple domain and multidomain MDM technology purpose-built to address the requirements of an MDM program that spans more than one data domain from a master data perspective. |
| Augmented MDM | The MDM solution should support the application of graph, machine learning and similar advanced technologies to MDM. Augmented MDM extends traditional MDM capabilities to reduce manual data management and governance tasks. |

B2C Customer Data

- This is the mastering of individual customer data (and other party data, such as citizen and patient data) during the process of creating trusted master records.
- It is common for B2C customer master data to be managed in a consolidation-style environment, where the entry points of the master data are not directly controllable by the MDM technology.
- An example of a B2C customer data use case is the mastering of customer data in support of business requirements such as a single view of a resident, 360-degree customer insights and a high-quality customer experience.

B2B Customer Data

- This is the mastering of institutional data during the creation of trusted master records that support processes for managing commercial relationships with organizations.
- Implementations enable the authoring of customer master data in workflow-, batch- or transaction-oriented processes that conform to one or more MDM implementation styles (or a hybrid of those styles). It is common for B2B customer master data to be managed in a workflow-oriented environment, where the entry points of the master data are controllable by the MDM technology.
- An example of a B2B customer data use case is the mastering of organizational customer data in support of business requirements such as account definition and management, a single view of the customer, 360-degree customer insights, and sales territory management.

Technical Use Cases for Master Data Management Solutions

150 of 191

Buy-Side Product Data

- This is the mastering of product or material data during the creation of trusted master records in support of business processes focused on supply chain management (SCM)

Sell-Side Product Data

- This is the mastering of product or material data during the creation of trusted master records in support of business processes for the provision of product data to customers.

Multidomain

- Critical data objects are mastered across multiple domains concurrently during the creation of trusted master records in support of business processes dependent on them.
- A master data domain encompasses related data entities that are of critical importance to an organization, such that they need to be mastered at the enterprise (as opposed to application) level to provide for semantic consistency across the business. These entities will prove central to how the organization does what it does; the actual observations represented by master data will be of significant interest to business executives — even if they do not use the term “master data.”
- Several patterns have emerged whereby “customer,” “party,” “product” or “thing” master data has become the highest priority for many organizations. The MDM solution should be capable of supporting all domains that are “in scope” for an MDM program, whether through client-driven or prepackaged data model styles, as defined by Gartner, or a combination of the two.

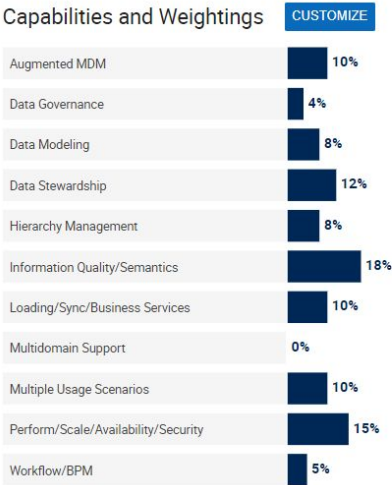
Use Case – B2C Customer Data

- The weightings are recommended by Gartner Research

B2C Customer Data

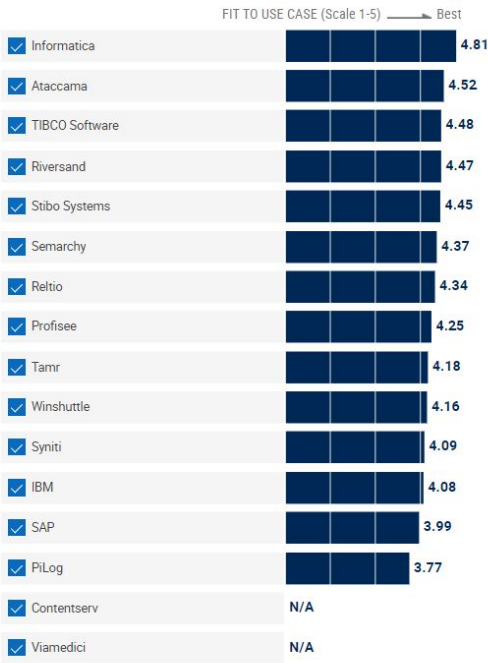
As of 19 November 2021

This is the mastering of individual customer data (and other party data, such as citizen and patient data) during the process of creating trusted master records.



Product Scores

Sort by score ▾



Ratings and summary scores range from 1.0 to 5.0:
1 = Poor or Absent: most or all defined requirements for a capability are not achieved
2 = Fair: some requirements are not achieved
3 = Good: meets requirements
4 = Excellent: meets or exceeds some requirements
5 = Outstanding: significantly exceeds requirements

Use Case – Multidomain

102 of 191

- The weightings are recommended by Gartner Research

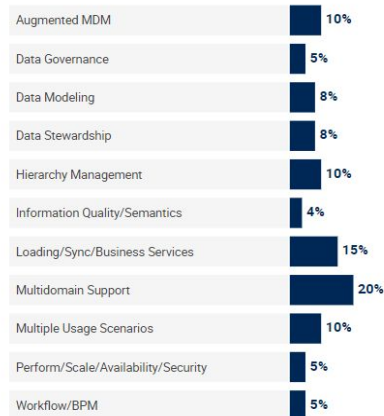
Multidomain

As of 19 November 2021

Critical data objects are mastered across multiple domains concurrently during the creation of trusted master records in support of business processes dependent on them.

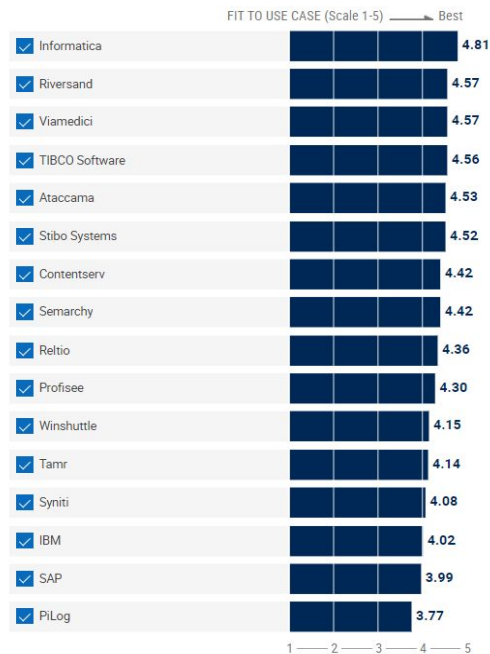
Capabilities and Weightings

CUSTOMIZE



Product Scores

Sort by score ▾



Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

Gartner Research ID G00746166

RESTRICTED DISTRIBUTION

102 © 2021 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

Representative MDM Systems Integrators (SI) Industry Experience

■ Manufacturing ■ Nonmanufacturing □ Not Represented

| ESP | Industry: Nonmanufacturing | | | | | | | | | |
|------------------------------|----------------------------|--------------------|----------------------------|--------|-------------|-------|----------------------|---------------|--------------------|-------------------------|
| | Healthcare | Financial Services | Distribution and Logistics | Retail | Hospitality | Media | Energy and Utilities | Public Sector | Telecommunications | Other Non-manufacturing |
| Accenture | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| ADVELLENCE | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Amplifi | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Apgar Consulting | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Business & Decision | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Camelot ITLab | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Capgemini | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Cognizant | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| First San Francisco Partners | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| HCL Technologies | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Infosys | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Infoverity | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Mastech InfoTrellis | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| parsionate | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| TCS | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Tech Mahindra | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| VIQTOR DAVIS | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| Wipro | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |

Source: Gartner

730144_C

RESTRICTED DISTRIBUTION

Metadata Management Critical Capabilities

Magic Quadrant for Metadata Management

105 of 191

Demand arising from a variety of data and analytics initiatives drives strategic requirements for metadata management solutions. This Magic Quadrant will help data and analytics leaders find the most appropriate vendor and solution for their organizational needs.

Quadrant Descriptions

Leaders

Leaders are frontrunners with offerings that support the full range of metadata management capabilities. They exhibit a clear understanding of, and vision for, where the market is headed, and are good at meeting customers' requirements for a variety of use cases.

Challengers

Challengers are well positioned in the light of key trends, but they may not provide the comprehensive breadth of functionality and support for use cases of the Leaders, or they may be limited to specific technical environments or application domains.

Visionaries

Visionaries demonstrate a strong understanding of emerging technology and business trends or have a position that is well aligned with current demand. However, they are not yet perceived as competitive players beyond their traditional customer base.

Niche Players

Niche Players have gaps in both their Completeness of Vision and Ability to Execute. They often exhibit a narrow focus in supporting particular use cases.



Gartner Research ID G00372820

RESTRICTED DISTRIBUTION

105 © 2021 Gartner, Inc. and/or its affiliates. All rights reserved.

© Gartner, Inc

Critical Capabilities for Metadata Management Platforms

106 of 191

| Critical Capability | Definition |
|-----------------------|--|
| Metadata repositories | Used by information managers to document and manage metadata, and to perform analysis using metadata. They can also use repositories to publish information about reusable assets that enables users to browse metadata during life cycle activities (such as design, testing and release management). |
| Business glossary | A repository used to communicate and govern an enterprise's business terms, along with the associated definitions and the relationships between those terms. |
| Data lineage | Specifies the data's origins and where it moves over time. It also describes what happens to data as it passes through diverse processes. Data lineage can help to analyze how information is used and to track key bits of information that serve a particular purpose. |
| Impact analysis | Conveys extensive details regarding the dependencies of information or the impact of a change within a data source. |
| Rule management | Automates the enforcement of business rules that are tied to data elements and associated metadata. This capability supports dedicated interfaces for creation, order of execution and links with information stewardship for effective governance. |

Critical Capabilities for Metadata Management Platforms (Cont.)

| Critical Capability | Definition |
|------------------------------------|---|
| Metadata ingestion and translation | <ul style="list-style-type: none">▪ Using techniques or bridges for various sources, such as:<ul style="list-style-type: none">– Extraction, transformation and loading (ETL)– Extraction, loading and transformation (ELT)– Application integration– Data integration– Insight engines– Business intelligence (BI) and reporting tools– Modeling tools– Database management system (DBMS) catalogs– ERP and other applications– XML formats– Hardware and network log files– Microsoft Excel spreadsheets and Word documents– PDF documents– Business metadata– Custom metadata▪ Vendors must be able to demonstrate the ability to identify, document and maintain relationships between ingested and translated metadata. |

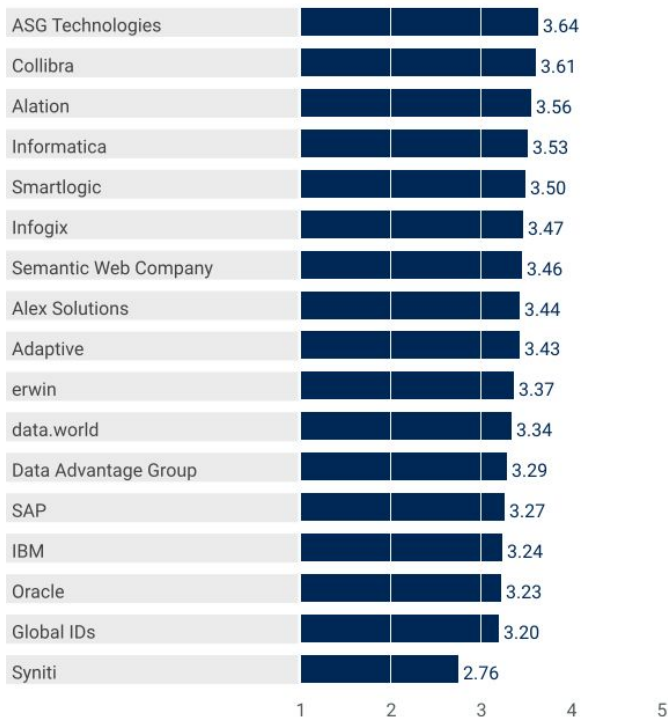
Use Cases for Metadata Management Solutions

108 of 191

Data governance

- Data governance use cases must support the situational application of policies and rules.
- Effectively governed metadata and content provide a glimpse into the workflow of data, including:
 - The ability to perform an impact analysis
 - A common data model
 - A business glossary
 - Accountability for terms and definitions
 - An audit trail for compliance

Product or Service Scores for Data Governance



As of 7 November 2019

© Gartner, Inc

Gartner Research ID G00378854

RESTRICTED DISTRIBUTION

108 © 2021 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

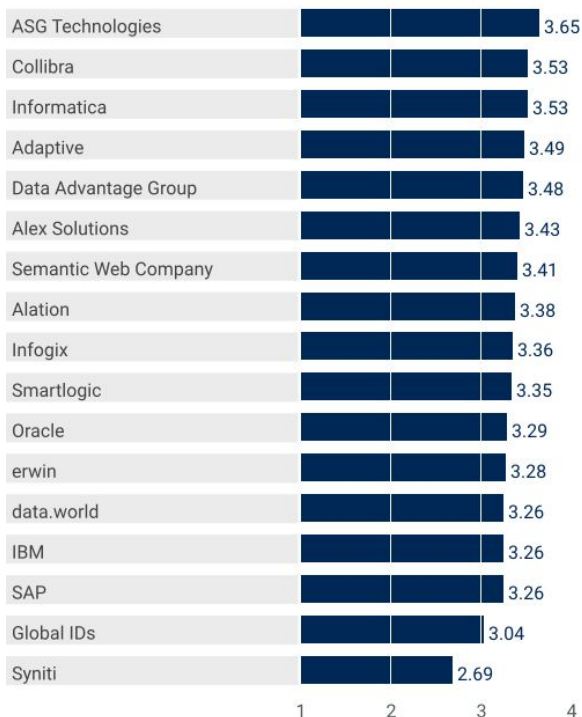
Use Cases for Metadata Management Solutions

109 of 191

Data risk and compliance

- The ability to identify data assets that represent some form of liability when they are exposed inadvertently or if there is no metadata trail to justify data usage.
- Demands mapping and identifying data assets, an understanding of data processing and its risks, the provision of data lineage and impact analysis, and ongoing data management. This includes security and risk professionals seeking to develop policies and controls for access to data via classification according to risk or security needs. The need for metadata management is reinforced by privacy requirements.

Product or Service Scores for Data Risk and Compliance



As of 7 November 2019

© Gartner, Inc

Gartner Research ID G00378854

RESTRICTED DISTRIBUTION

109 © 2021 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

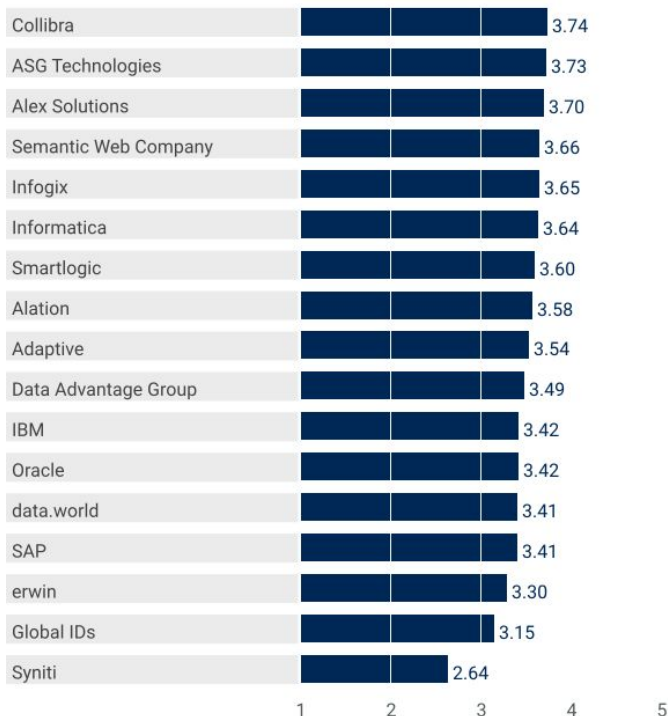
Use Cases for Metadata Management Solutions

110 of 191

Data analysis

- Metadata management provides insights into the uses of data for data analysis.
- Requirements for this use case include:
 - Discovering and inventorying data
 - Leveraging known uses of data
 - Learning through a community of users
 - Lineage and impact analysis for monitoring data provenance
 - Guiding change management.
 - The objective of this use case is to support the building of a data catalog for analytical uses of data across an organization.

Product or Service Scores for Data Analysis



As of 7 November 2019

© Gartner, Inc

Gartner Research ID G00378854

RESTRICTED DISTRIBUTION

110 © 2021 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

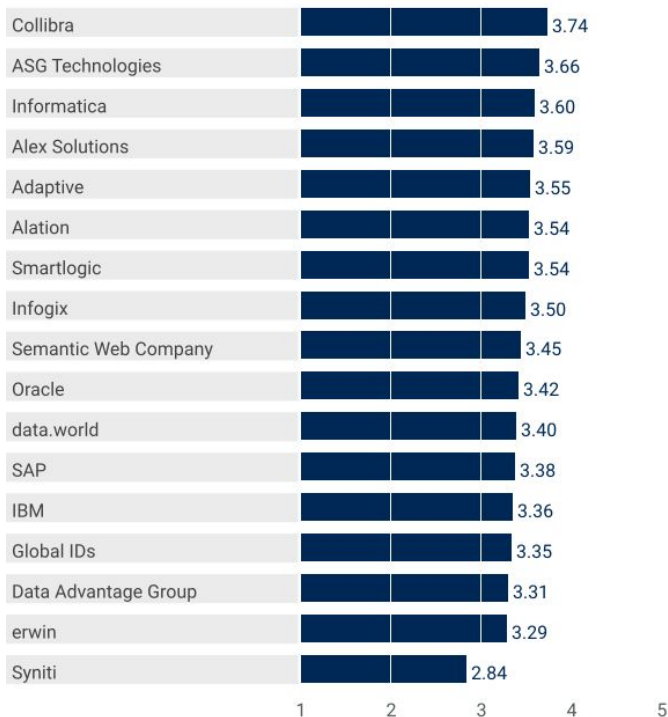
Use Cases for Metadata Management Solutions

111 of 191

Data value

- The use of metadata to inventory, assess and analyze data assets to quantify their value.
- This use case focuses on the future. Metadata and data is analyzed for current and potential value-add, including the identification of additional metadata capturing or additional datasets for enrichment. It leverages support for data valuation methodology.

Product or Service Scores for Data Value



As of 7 November 2019

© Gartner, Inc

Gartner Research ID G00378854

RESTRICTED DISTRIBUTION

111 © 2021 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

Best Practices with PII

Engagement #: 330079673 | Version 1



COLORADO
Governor's Office of
Information Technology



01

Example Best Practices – State PII Organization

Pages 3 - 12



02

Structuring a PII Data Program

Pages 13 - 16



03

Next Steps








Pages 17 - 19

Best Practices for State PII Management

Example State PII Best Practices

115 of 191

Below are best practice examples taken from other States and large local government bodies with multiple agencies and departments. These can be used to inform the Data Governance structure and practices for the State of Colorado's OIT Personally Identifiable Information program governance.

|  Change Management |  Data Literacy and Education |  Data Governance |  Data Usability |  Data Set Maintenance |  Data Source Identification |  Security |
|--|---|--|--|---|---|---|
| <ul style="list-style-type: none">• Create knowledge that data is a shared, strategic asset.• Share stories around other states and worldwide efforts for shared data structures. | <p>Provide Agencies with an example schedule for data dictionary review so that personnel understand data structure within each Agency.</p> | <ul style="list-style-type: none">• Require data governance from accountable entities within each Agency or State Department.• Ensure that the data governance structure matches the technology solution. | <ul style="list-style-type: none">• Validate that data is reusable.• Ensure that data is interoperable. | <ul style="list-style-type: none">• Verify that each data set provides new insights and that data sets are not repeated, especially within Agencies.• Ensure that a set schedule for maintenance exists, or at least guidelines from the state on data retention and disposal. | <ul style="list-style-type: none">• Ensure that data sources are known for PII, and integration maps are created for this information, especially for external use of PII.• Provide Agencies with an example of a data dictionary and ask them to create one for each data set containing PII. | <ul style="list-style-type: none">• Ensure data is secured and protected.• Define security and risk governance by deciding what is acceptable risk and how to enable risk control• Map and Monitor all data access privileges provided to application users, developers, etc. |

Change Management Drives Change Success

116 of 191

Leadership must support transformation and organization design initiatives that ensure processes and structures fit changing needs

Change Management Approach



Top-Down Change

- Use open-source approach that involves employees in the change process and empowers the enterprise.
- Engage the workforce as active participants in change decisions by including employees as co-creators of change decisions.
- Shift ownership of change planning to teams and employees by calling on them to create their own personal change implementation plans.
- Refocus change communication on open conversations by encouraging employees to talk freely about change.

Gartner reference ID G00766030

RESTRICTED

Set the
Strategy and
Define the
Vision

Leaders Set the Change Strategy

Leaders alone determine the strategic changes the organization will make and the vision for those changes.

Plan
Implementation

Leaders Own Implementation Planning

Leaders create implementation plans indicating what employees should do.

Communicate
and Sustain
Change

Organizations Roll Out Communication Campaigns

Organizations roll out communication campaigns to tell employees about the change and its benefits.



Open-Source Change

Employees Co-Create Change Decisions

Engage the workforce as active participants in making and shaping change decisions.

Employees Own Implementation Planning

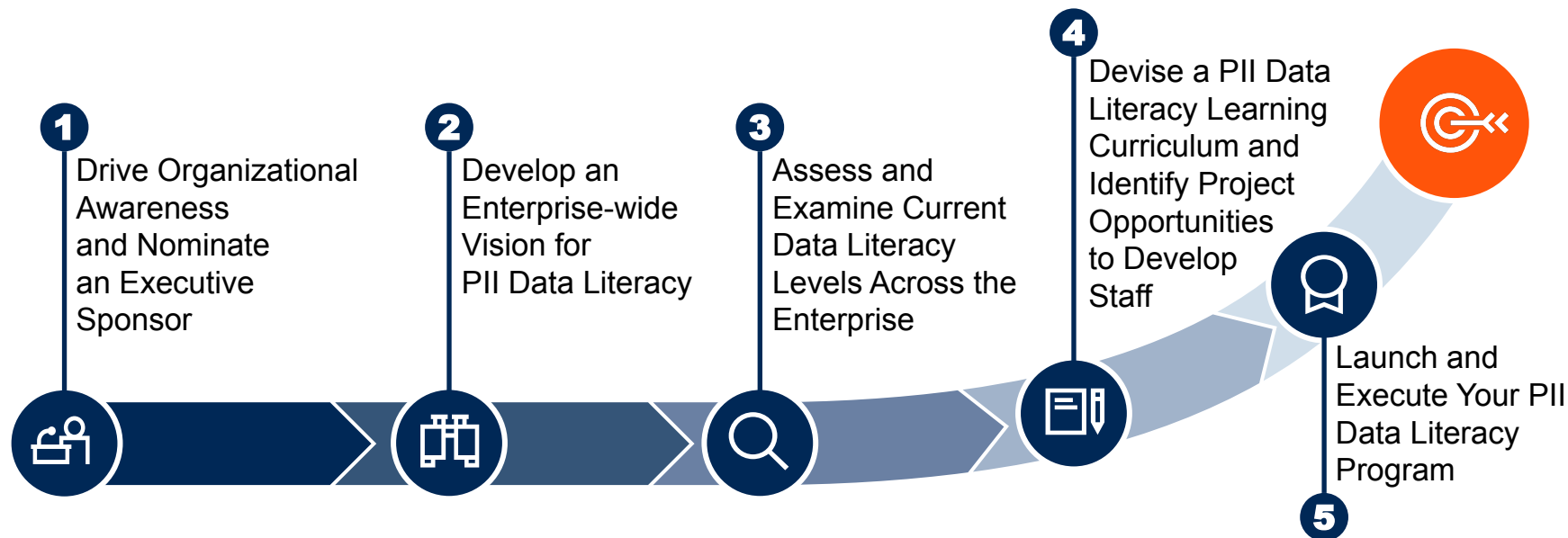
Shift ownership of change planning to employees to create personal change implementation plans.

Employees Talk Openly About Change

Refocus change communication on open conversations.

5 Steps to Building a Data-Literate Organization

117 of 191



- **Broad definitions of PII and personal data are evolving to cover more and more kinds of data and differences between the two are becoming less distinct.**
- **Data literacy enables business users to understand what PII data is available to them, how it can be used, and what its limitations may be. They must know how PII data from different sources can be combined, or how it might be enriched with trusted information from third parties.**

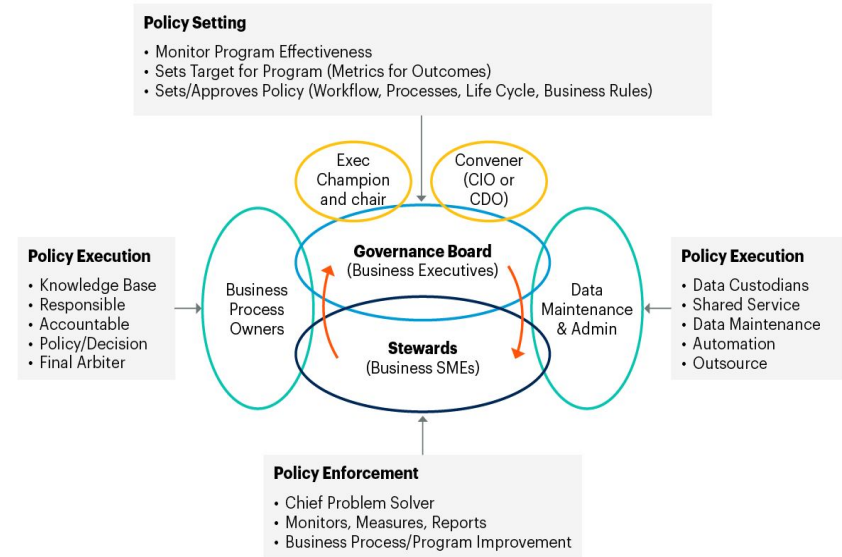
Governing PII and other critical data requires orchestration of resources and attention from D&A business stakeholders, IT, privacy and information security

118 of 191

To start driving data and analytics governance CDO's should:

- Drive business PII relevance, actionability and business value by using organizational structure to your advantage. Create high-functioning, cross-functional teams for data and analytics governance.
- Focus on PII-specific business outcomes from the beginning by determining how the least amount of data can have the biggest impact on business outcomes.
- Maximize impact and business outcomes by appointing the chair, or co-chair, for any data and analytics governance committee based on who cares most.
- Build and sustain momentum by starting with key PII data element definitions and use tools to help engage and enable the participants.

Data and Analytics Governance Functions and Roles



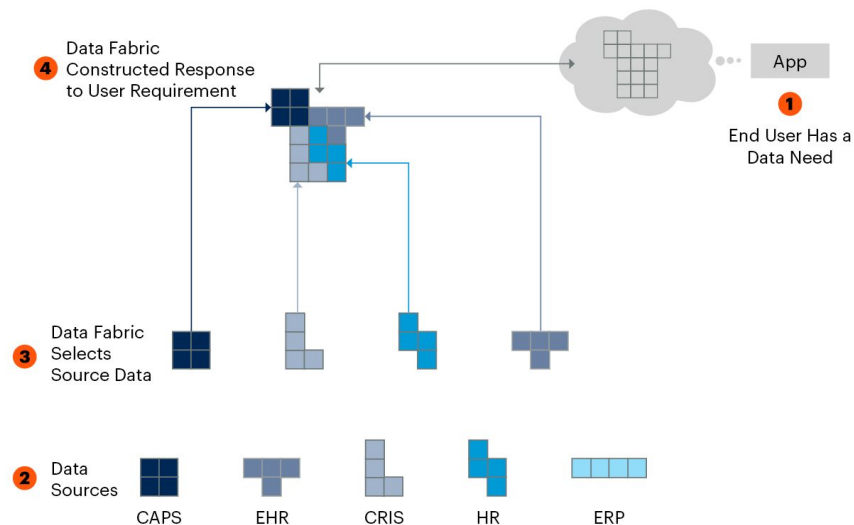
Source: Gartner
745960_C

The data fabric offers an advanced solution for data interoperability and usability

119 of 191

- Many organizations lack a baseline understanding of how data is currently used.
- Data fabric is enabling the continuous understanding of PII data usage, known as metadata management.
- The metadata — observable information regarding your data assets — creates an emergent design for data flows, integration concepts and data object development. It even defines the PII data demand model.
- Helps solve some of the interoperability issues with PII data by acting as the single-pane-of-glass access point to disparate sources of data truth.

Data Fabric Basics



Source: Gartner March 2022

CAPS = core administrative processing solution; EHR = electronic health record; CRIS = clinical research information system; HR = human resources; ERP = enterprise resource planning

765001_C

Data assets are critical to the success of all strategic business imperatives, the quality of those assets must become of paramount concern for data and analytics leaders



Accessibility:

Data is available, easily retrieved and integrated into business processes



Accuracy:

Data value accurately reflects real-world objects or events that the data is intended to model



Completeness:

Records are not missing fields and datasets are not missing instances



Consistency:

Data that exists in multiple locations is similarly represented and structured



Precision:

Data is recorded with precision required by business processes



Relevancy:

Data is applicable to one or more business process or decision



Timeliness:

Data is updated with sufficient frequency to meet business requirements



Uniqueness:

Each data record should be unique based on how it is identified



Validity:

Data conforms to the defined business rules/requirements and comes from verifiable source

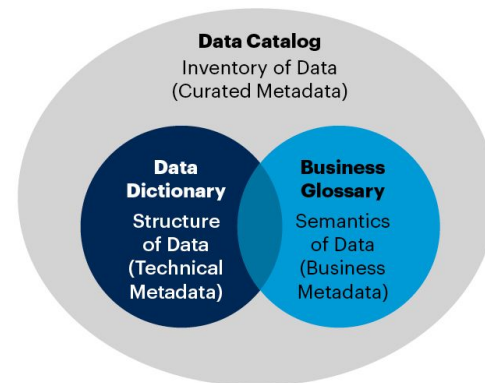
Integrity, Interpretability, Reliability, Usability, Objectivity ...

Know your data and define data quality requirements, rules, metrics and expected business outcome with stakeholders.

Data dictionaries, business glossaries and data catalogs serve specific purposes in managing data. Each of them expresses different aspects and usage of metadata

- A data dictionary (technical metadata) is a collection of names, definitions and attributes about data elements that are being used or captured in a database, information system or research project. It describes the meanings and attributes of data elements within the context of a project and provides guidance on interpretation, accepted meanings and representation.
- Business glossary (business metadata) is a collection of business terms and definitions across business domains, providing common understanding over data elements for all business operations. It facilitates governance policy analysis and development and supports taxonomies and ontologies to address semantic variations.
- Collecting state-wide business terms and definitions of PII elements will help with standardizing specific critical data element definitions as a component of a metadata management solutions will maintain a glossary of all incorporated data elements.
- A data catalog (curated metadata) is a collection of metadata to create, curate and maintain an inventory of data assets through the discovery, description and analysis of datasets. It enables data consumers to find and understand relevant datasets to extract business value from data. Data in a data catalog can contain any type of data in all conditions, either trusted/untrusted or governed/ungoverned.

Data Dictionary, Business Glossary, and Data Catalog



Source: Gartner
754031_C

Data security governance framework used to mitigate business risks caused by security threats, data residency & privacy issues.

Creation of data security management framework, control catalogs and processes seamlessly integrated with data security and data governance could be strenuous but necessary to support business operations while implementing appropriate data security and privacy controls to mitigate business risks. The Gartner Data security governance (DSG) framework can be used in conjunction with other international and local standards to develop fit-for-purpose data security charters, control catalogs and processes

Relationship Between Data Security Management Frameworks, Control Catalogs and Processes



Source: Gartner
775485_C

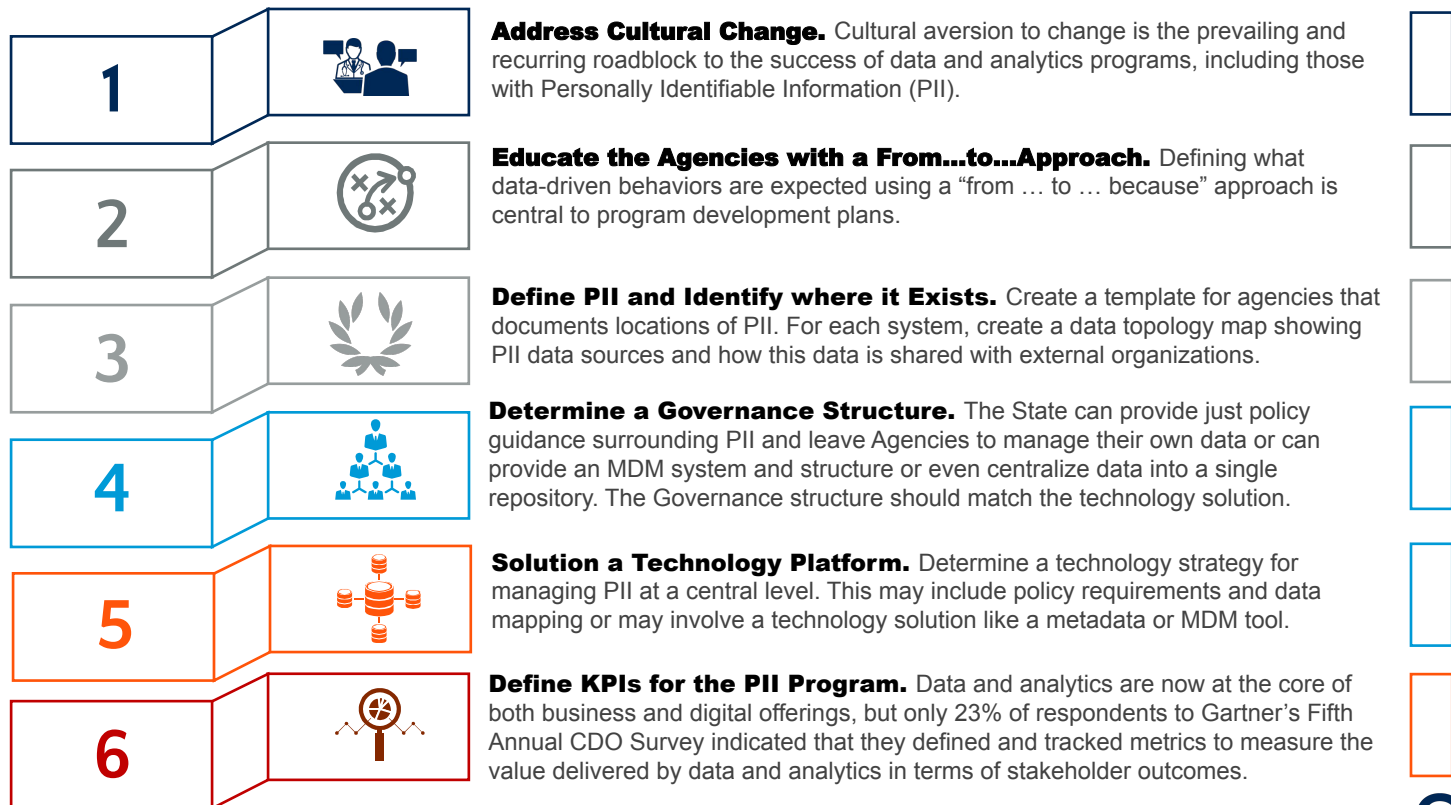
Gartner.

Structuring a PII Data Program

Structuring a PII Data Program - Notes from Gartner Research

124 of 191

The below steps are notes from Gartner Research which can be used to structure the State of Colorado's PII Program.

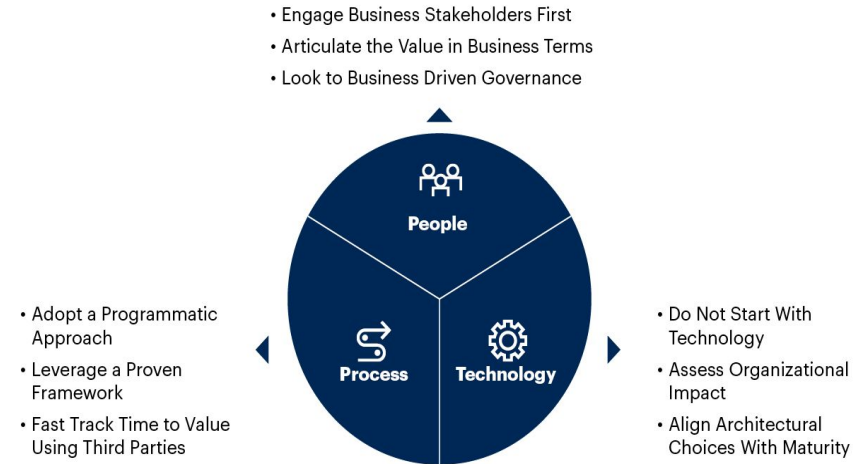


RESTRICTED

An MDM framework has helped clients structure their enterprise data sets from the perspective of the people, process and technology pillars

- Clearly define and articulate the links between the MDM program and the business outcomes it supports, taking a programmatic approach to MDM by leveraging proven frameworks that map out the journey.
- Lay a solid foundation for success by engaging business stakeholders early to agree upon the prioritized business outcomes their MDM program will support, and to secure support for a business-driven information governance team.
- Adopt an MDM architecture most suited to fulfill their current and future goals by learning the distinct characteristics of the different MDM implementation styles and their impacts on existing business processes.

MDM Essentials Across People, Process and Technology



Source: Gartner
730039_C

Gartner

Gartner

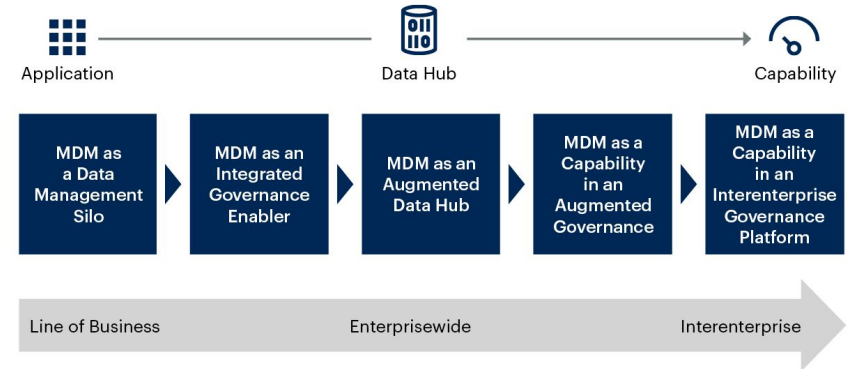
RESTRICTED

MDM solutions will evolve over time to improve business processes and help with the governance of critical data elements

When successfully executed, a combination of forward-thinking MDM strategies, MDM best practices and new technologies are allowing data and analytics leaders to:

- Improve the trustworthiness and scale of MDM processes by utilizing active metadata to automate the creation and management of master data governance rules, and to right-size the scope of MDM programs
- Benefit from the insights and economies of scale that exist when treating master data as a shared asset across corporate boundaries
- Extend the value and insights of MDM programs by utilizing graph and similar technologies to identify previously unknown relationships that may themselves be considered master data
- Optimize and automate MDM and governance business rules by integrating the insights from augmented data quality solutions
- Scale data stewardship processes both through the use of active metadata to identify exceptions and through the use of AI to automatically resolve exceptions.
- Inform and automate MDM-related data integration patterns by utilizing insights from augmented data integration solutions, implementing MDM within an overall data fabric design
- Support more adaptive, context-centric forms of data governance

The Evolution of MDM



Source: Gartner
753647_C

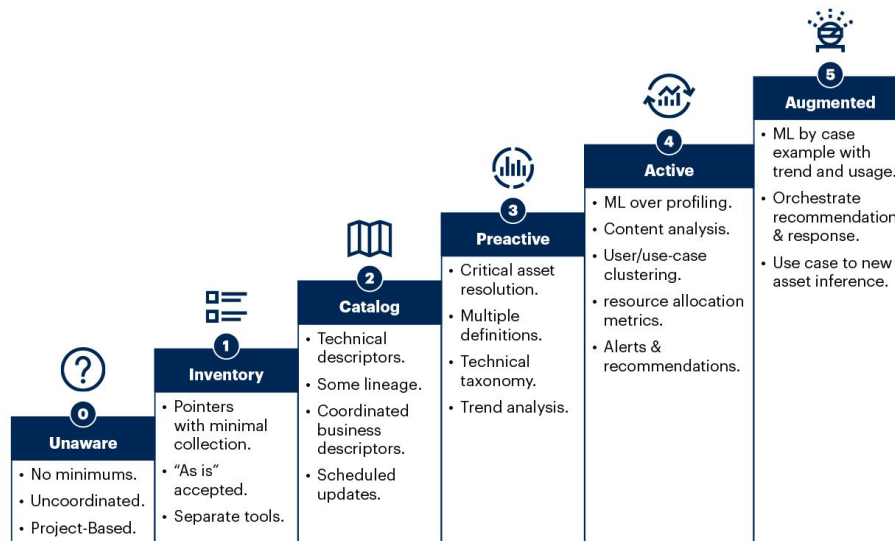
Gartner

While Master Data Management will help structure enterprise data sets, Metadata Management can offer insight into its usability, access, and other business critical attributes

Data and analytics leaders engaged in data management solutions initiatives must address active metadata and:

- Determine the gap between current state metadata management and the target state by cataloging currently available metadata and comparing the metadata inventory to its usage.
- Deliver advanced metadata management capabilities by focusing on priority data domains that cross business areas to assist in a phased approach to metadata-enabled data management.
- Evaluate team member skills and any tools in use to resolve the metadata management maturity or skill gaps.
- Develop separate tactics for different metadata requirements by comparing active metadata requirements from broad enterprise to localized needs.

Metadata Management Technology Maturity



Source: Gartner
736613_C

Next Steps

Structuring the PII Program within the Agencies

129 of 191



1. Create a high-level operating model for what OIT handles and what the Agencies do currently and what they need to do in the future
2. Identify the Data and Analytics roles that may be needed by the Colorado Agencies for PII Management
3. Document how these roles work with the existing governance structure, future leadership (Chief Privacy Officer, CDO and CISO) the PII Advisory Board and GDAB.
4. Pull legal experts to review
5. Create an opt-in model for a metadata management or Master Data Management system.
6. Create roles and responsibilities for each role. Include the tasks each role will perform, and skills required.
7. Create a D&A maturity assessment the CDO can offer for each agency. Would need to survey both IT and business resources for each Agency and provide a roadmap to improve their maturity and let them retake annually.

RESTRICTED

Next Steps

130 of 191

- 1 Discussion surrounding best practices and next steps.
- 2 Gartner will provide the PII Solution Architecture deliverable, outlining several options for a technology solution to more effectively manage PII, including metadata and Master Data Management (MDM) systems.



RESTRICTED

Bharat Bagaria

Expert Partner
Gartner Consulting
Phone: +1 916 210 0907
Email: bharat.bagaria@gartner.com

Chelsea Wyatt

Senior Managing Partner
Gartner Consulting
Phone: +1 303 590 8599
Email: chelsea.wyatt@gartner.com

Farhat Naweed

Senior Director
Gartner Consulting
Phone: +1 475 685 5848
Email: farhat.naweed@gartner.com

Nikhil Nayak

Associate Director
Gartner Consulting
Phone: +1 916 213 7447
Email: nikhil.nayak@gartner.com

Lauren Talyor

Account Executive
Gartner
Phone: +1 205 837 3693
Email: lauren.talyor@gartner.com

PII Needs Analysis Report – Security Assessment Framework

Engagement #: 330079673 | Version 1



COLORADO
Governor's Office of
Information Technology

Contents

133 of 191



01

Executive Overview and Document Purpose

Pages 3 - 5



02

Security Assessment Framework

Pages 6 – 16



03

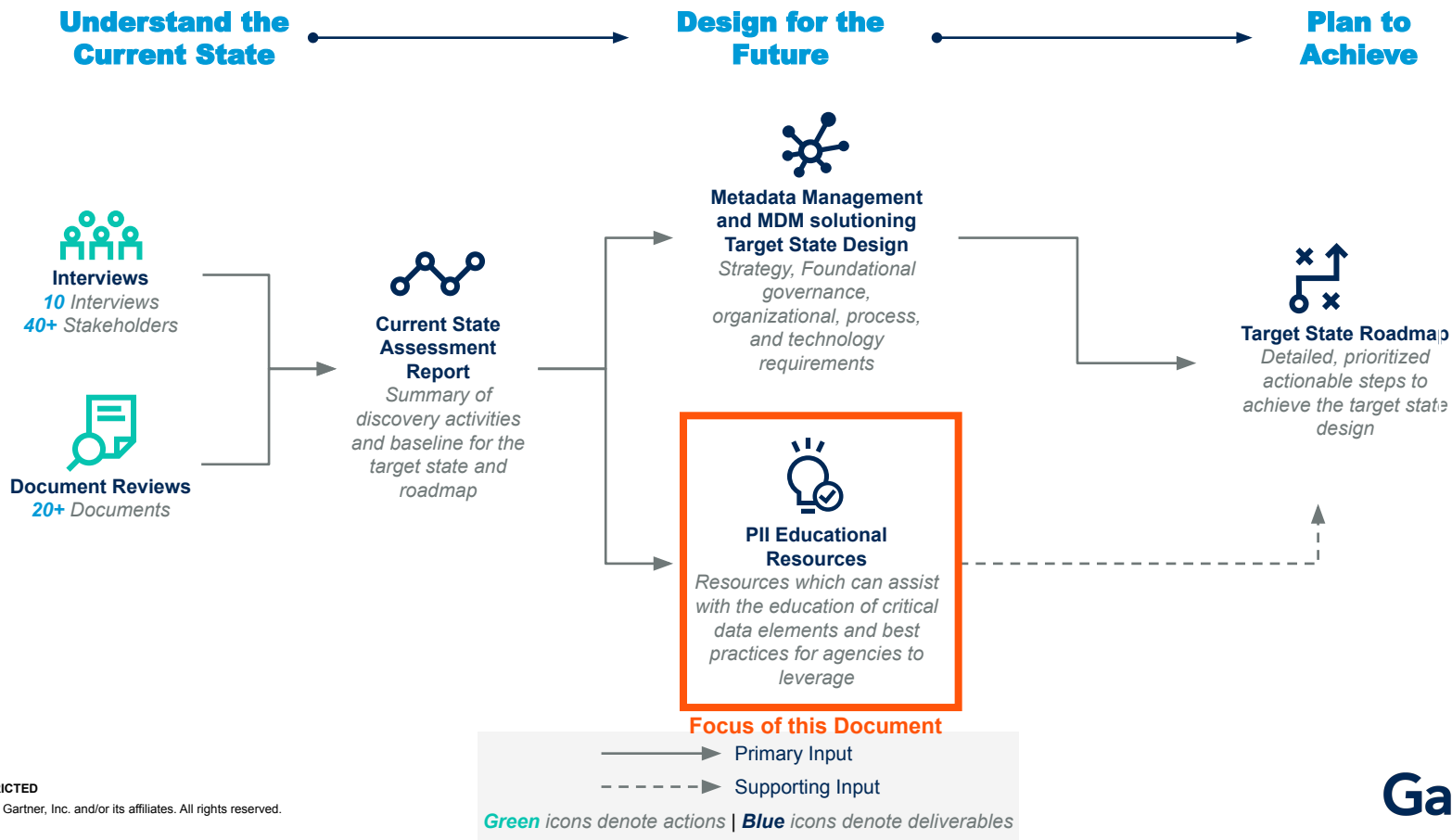
Appendix

Pages 17 – 26

RESTRICTED

Executive Overview

Gartner Engagement Overview – PII Solution Architecture



This engagement was initiated to address House Bill 21-1111

136 of 191

Legislator ask:

- Study **where personally identifiable information is stored** by state agencies throughout Colorado
- Identify entities that have **access** to personally identifiable information stored by state agencies
- **Determine the costs and processes** necessary to centralize the storage and protection of personally identifiable information
- Study to be completed and presented to the Joint Technology Committee(JTC) on or before **01/01/2023**
- Personally identifiable information means **information that may be used, along or in conjunction with any other information**, to identify a specific individual. Some examples can be found to the right.

Personally identifiable information

Personally identifiable information means information that may be used, along or in conjunction with any other information, to identify a specific individual, including but not limited to:

- Name
- Date of birth
- Place of birth
- Social security number
- Tax identification number
- A password or passcode
- Official government-issued driver's license or identification card number
- Information contained in an employment authorization document
- Information contained in a permanent resident card
- Vehicle registration information
- License plate number
- Photograph
- Electronically stored photograph, or digitized image
- Fingerprint
- Record of a physical feature
- Physical characteristic
- Behavioral characteristic
- Handwriting
- Government passport number
- Health insurance identification number
- An employer, student, or military identification number;
- Financial transaction device
- School or educational institution attended;
- Source of income
- Medical information
- Biometric data
- Financial and tax records
- Home or work addresses or other contact information
- Family or emergency contact information;
- Status as a recipient of public
- Assistance or as a crime victim
- Race
- Ethnicity
- National origin
- Immigration or citizenship status
- Sexual orientation
- Gender
- Identity
- Physical disability
- Intellectual and developmental
- Disability
- Religion

RESTRICTED

Security Assessment Framework

Data security governance framework used to mitigate business risks caused by security threats, data residency & privacy issues.

Creation of data security management framework, control catalogs and processes seamlessly integrated with data security and data governance could be strenuous but necessary to support business operations while implementing appropriate data security and privacy controls to mitigate business risks. The Gartner Data Security Governance (DSG) framework can be used in conjunction with other international and local standards to develop fit-for-purpose data security charters, control catalogs and processes

Relationship Between Data Security Management Frameworks, Control Catalogs and Processes



Data Risk Assessments focus security initiatives at the appropriate level to detect and mitigate data risks.

- Many organizations prioritize data security around identification and management of critical information.
- To ensure compliance and security protocol are upheld, Colorado can focus security initiatives on the assessment of business processes which contain PII or other critical data elements.
- The assessments can help identify potential data risks which are not mitigated and their broader affect on the business processes.
- Engage with business stakeholders to identify internal and external factors can help determine the selection of security frameworks, controls, or mitigation pathways.
- Colorado has already begun with steps 1 and 2 with established security controls and governance processes.

A Risk-Based Approach for Data Security Programs Set Up

Step 1: Establish Data Security Governance and Management Function

- Create a data security steering committee
- Set up data security management function and a dedicated data security manager
- Formalize data security management frameworks, control catalogs and security processes

Step 2: Streamline Data Discovery and Classification

- Include structured and unstructured data on-premises and in the cloud
- Prioritize sector-specific classification standards
- Adopt modern classification approaches and automation technologies

Step 3: Operationalize Data Risk and Compliance Assessment Processes

- Apply data risk assessment (DRA) to evaluate effectiveness of data security and privacy controls
- Utilize financial data risk assessment (FinDRA) to prioritize investments
- Perform mandatory data security compliance assessments

Step 4: Apply Consolidation Approach to Integrate Siloed Data Security Products

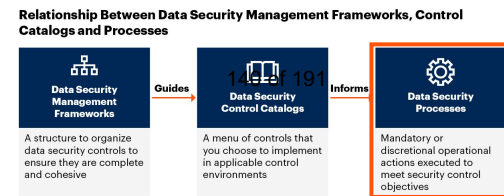
- Select data security products with higher integrability with heterogeneous platforms
- Prioritize the broad-spectrum DSPs than the specialized DSPs

Use an Iterative Feedback Loop at Each Step to Prioritize Data Risk Treatment Plan

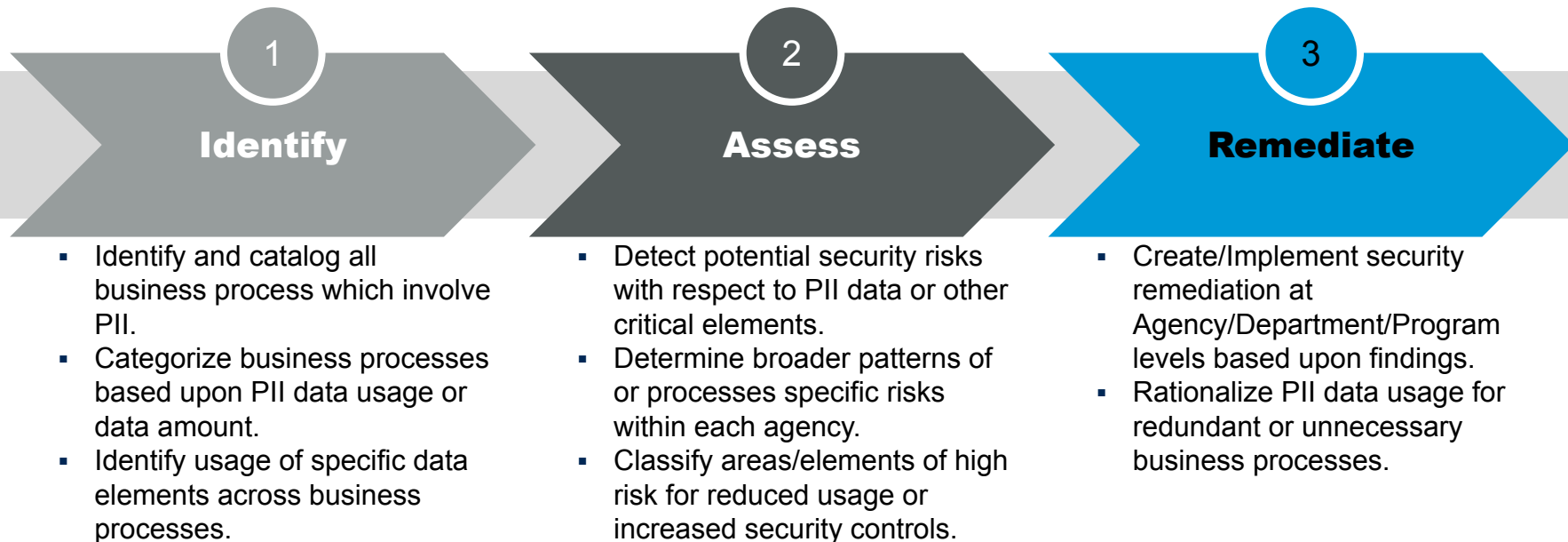


Source: Gartner
775485_C

Data Security Processes: Data Risk Assessments

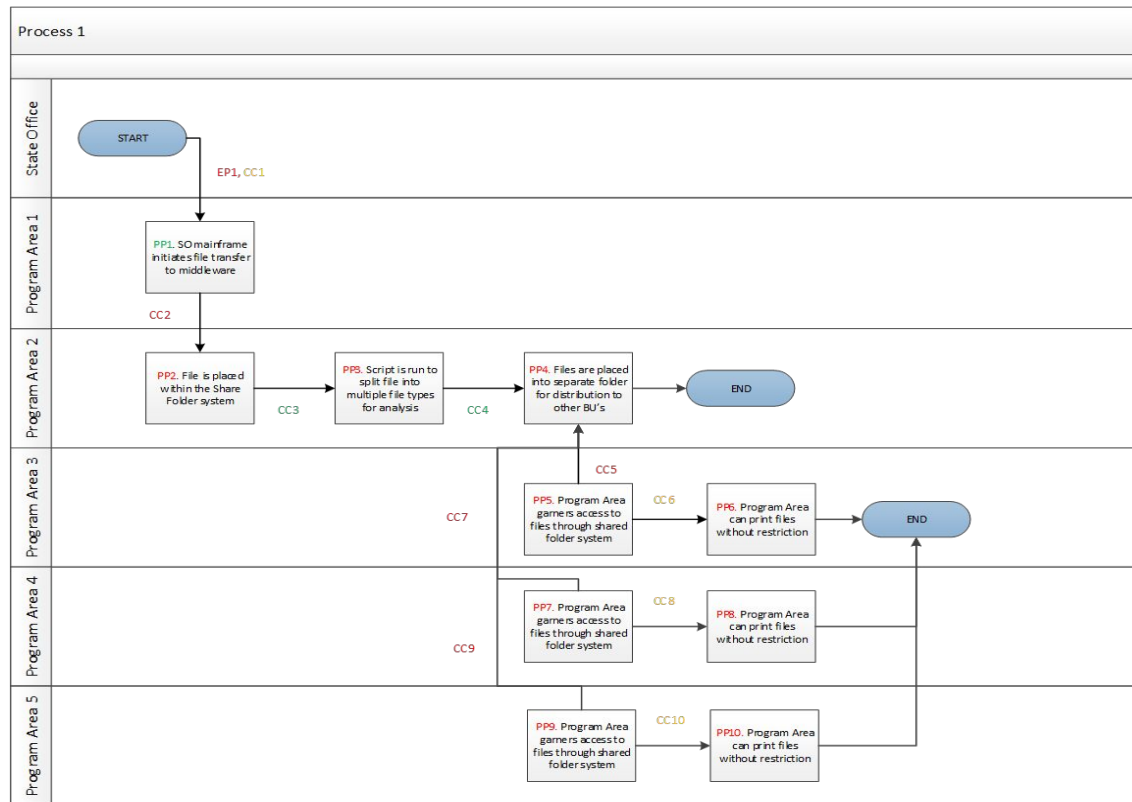


As part of its ongoing security processes, CO-OIT and other Colorado agencies can implement a Data Risk Assessment process to identify, assess, and remediate potential security risks or existing issues with respect to PII or other critical data elements.



Each Business Process which contains PII or other critical elements can be assessed to ensure data security 141 of 191

- Business Process which leverage PII or other critical data elements should be documented.
- Potential data security risks can be identified within each business process
- Processes which undergo changes yet remained undocumented would have require assessment and evaluation for potential risks
- CO-OIT and other Colorado agencies must direct process changes through established change management/governance processes to capture the necessary information and ensure processes change appropriately



Data Risk Assessment Framework

142 of 191

Gartner's Data Risk Assessment framework is designed to identify potential security risks related to PII or other critical data elements. The Assessment Framework can incorporate a scoring logic stemming from Gartner Research and industry best practice. The Data Risks Assessment Framework will assess business processes across 3 specific domains:

Domain

Description

Key Assessment Areas



Communication Channels

- Communication Channels indicate data in motion and security attributes of PII or other critical data elements in transit. Communication channels will govern the directionality and methodology of those data elements.

- Communication Channels focus on security attributes related to the transfer critical data between systems, people, application, or databases.



Process Points

- Process Points indicate the specific event which occurs during a business process where PII or other critical data is manipulated or leveraged to continue the overall process to a specific outcome. Each Process Point can reside within a specific application, user group, or database where the defined event is occurring.

- Process Points focus on the security attributes of the system, person, application, or database where the data is housed or manipulated.



Entry/Exit Points

- Entry/Exit Points indicate the area where PII or other critical data elements cross the CO-OIT or Colorado agency network boundaries and are sent to or from an external entity.

- Entry/Exit Points evaluate the method, amount, and directionality of PII or other critical data elements traversing network boundaries or when shared with other partner institutions.

RESTRICTED

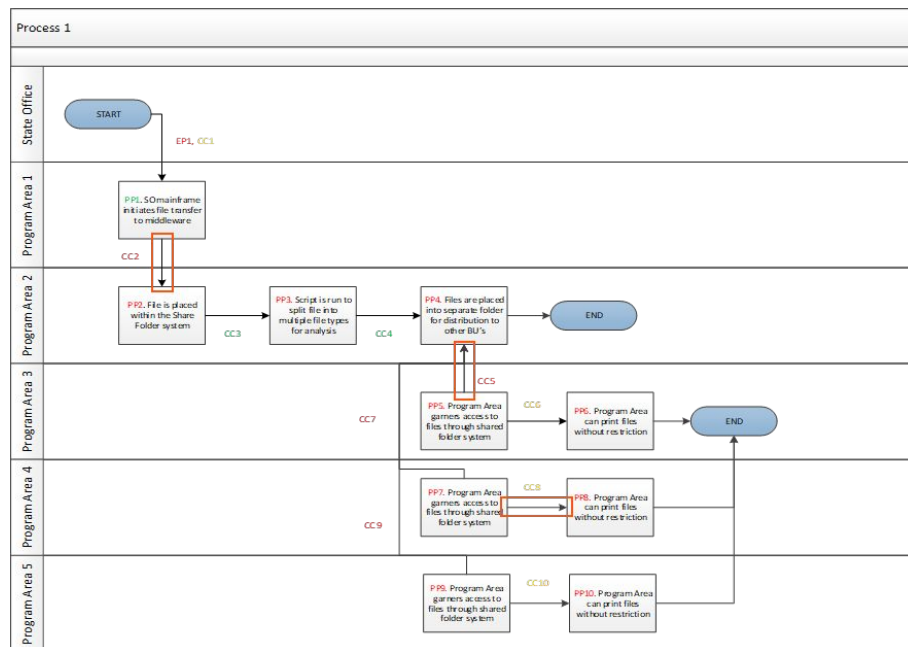
Communication Channel – Assessment Attributes

143 of 191

Communication Channels describe specific steps transfer of information between individual process steps within a business process. These steps represent when data is motion within throughout the business process either within or outside of the infrastructure.

Communication Channels can be evaluated for various attributes to determine potential data security risks. These attributes include but are not limited to:

| Attribute | Definition |
|------------------------|--|
| Existence | Identifies whether PII data elements are incorporated as part of the Communication Channel |
| Encryption | Identifies the existence of encryption of the Communication Channel |
| Encryption Type | Identifies the type of encryption leveraged within the Communication Channel |
| Authentication | Determines if individuals are required to log into a system/application to initiate potential communication channels which contain PII data elements |
| Authorization | Determines how individual rights permissions are granted to those who are exposed to PII data elements for that Communication Channel |
| Audit | Determines the existence of an audit trail for data in motion for each Communication Channel |
| Initiation | Identifies whether the transmission of PII Data Elements information is system initiated, manually initiated, or a combination of the two |



RESTRICTED

Communication Channel – Assessment Interview Questions^{144 of 191}

As each agency conducts Data Risk Assessments, Communication Channels can be evaluated by leveraging a set of interview questions during business process assessments. These questions include but are not limited to:

- Which PII Data elements are contained within this communication channel
- How is the communication channel initiated?
- Is the initiation of the communication channel automatically or manually triggered?
- Is this communication channel contained within the system/application which is currently being used?
- Does the communication channel span multiple systems/applications?
- What is the communication type? (phone, email, mail, application notification, etc.)
- Is this communication channel encrypted?
- What is the level of encryption for this communication channel
- Do users need to authenticate within the system/application prior to initiating this communication channel?
- Do users require authorization to initiate this communication channel?
- Is this communication channel audited or recorded by the system/application?

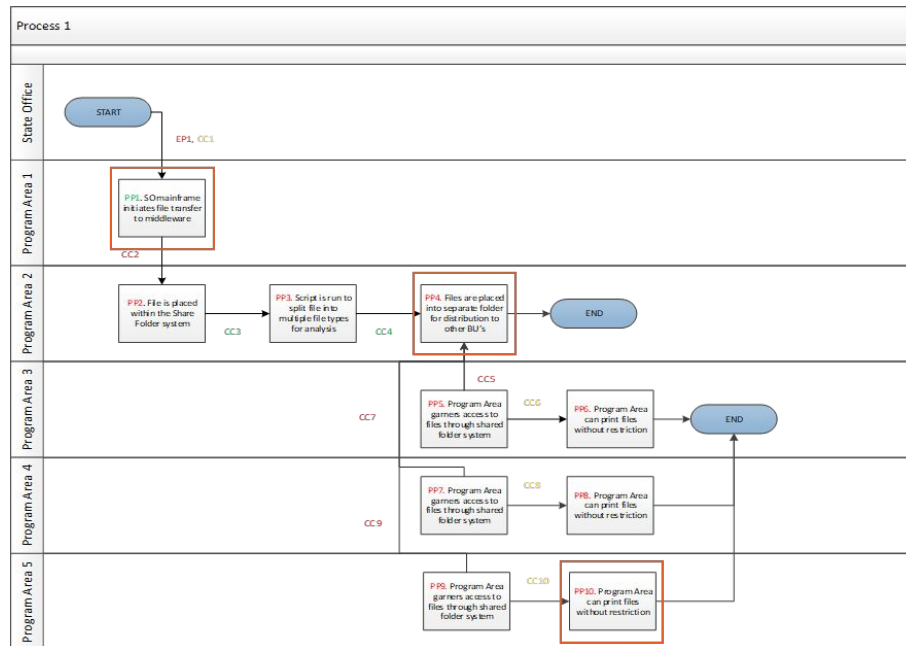
Process Points – Assessment Attributes

145 of 191

Process Points describe specific steps within a business process where PII data or other critical elements are at manipulated or at rest within an infrastructure

Process Points can be evaluated for various attributes to determine potential data security risks. These attributes include but are not limited to:

| Attribute | Definition |
|------------------------|--|
| Existence | Identifies whether PII data elements are incorporated as part of the Process Point |
| Incorporation | Identifies whether additional PII data elements are introduced which were not present from the previous Process Point |
| Encryption | Identifies the existence of encryption of the Process Point |
| Encryption Type | Identifies the type of encryption leveraged within the Process Point |
| Authentication | Determines if individuals are required to log into a system/application to initiate potential Process Points which contain PII data elements |
| Authorization | Determines how individual rights permissions are granted to those who are exposed to PII data elements for that Process Point |
| Audit | Determines the existence of an audit trail for data in motion for each Process Point |



RESTRICTED

Process Points – Assessment Interview Questions

146 of 191

As each agency conducts Data Risk Assessments, Process Points can be evaluated by leveraging a set of interview questions during business process assessments. These questions include but are not limited to:

- Which PII Data elements are contained within this Process Point?
- Which application/system(s) does this specific process point leverage?
- Is this process point contained within the system/application which is currently being used?
- Does the process point span multiple systems/applications?
- Is this application/system encrypt data at rest?
- What is the level of encryption utilized?
- Do users need to authenticate within the system/application prior to completing this process step?
- Do users require authorization to initiate this process point?
- Is this process point audited or recorded by the application/system(s)?

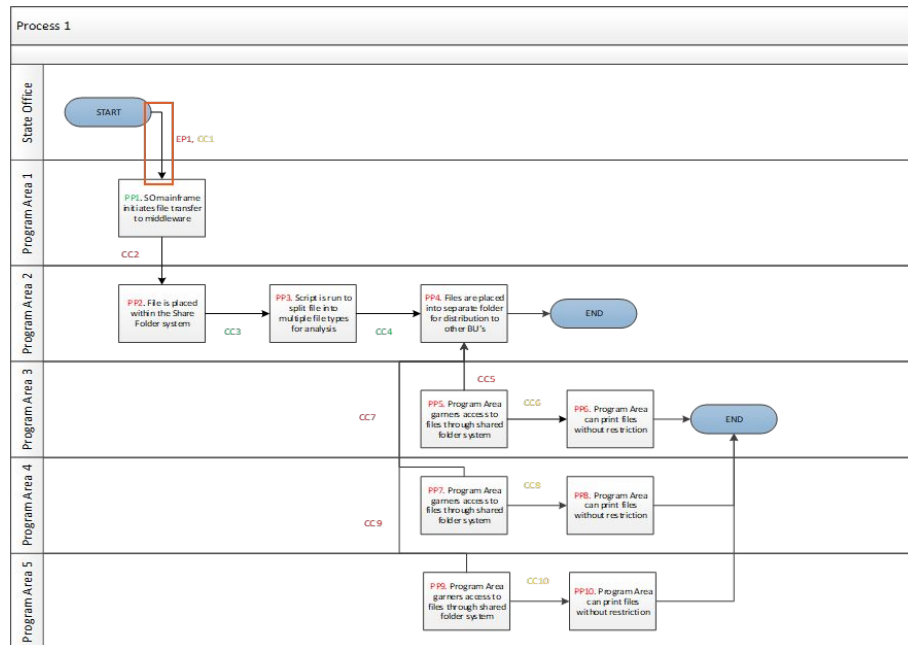
Entry/Exit Points – Assessment Attributes

147 of 191

Entry Points describe specific areas where data enters/exits an environment. These points represent areas of ingress/egress within the infrastructure and characteristics of that ingress/egress.

Entry/Exit Points can be evaluated for various attributes to determine potential data security risks. These attributes include but are not limited to:

| Attribute | Definition |
|-----------------------|--|
| Existence | Identifies whether PII data elements are incorporated as part of the Entry/Exit Point |
| Identification | Determines which PII data elements are incorporated as part of the Entry/Exit Point |
| Directionality | Determines whether PII data elements are inbound or outbound for each Entry/Exit Point |
| Amount | Identify the amount of PII data elements and amount of data which is incorporated as part of the Entry/Exit Point |
| Data Format | Determines if individuals are required to log into a system/application to initiate potential Process Points which contain PII data elements |
| Data Agreement | Determines how individual rights permissions are granted to those who are exposed to PII data elements for that Process Point |
| Frequency | Determines the existence of an audit trail for data in motion for each Process Point |



RESTRICTED

Entry/Exit Points – Assessment Interview Questions

148 of 191

As each agency conducts Data Risk Assessments, Entry/Exit Points can be evaluated by leveraging a set of interview questions during business process assessments. These questions include but are not limited to:

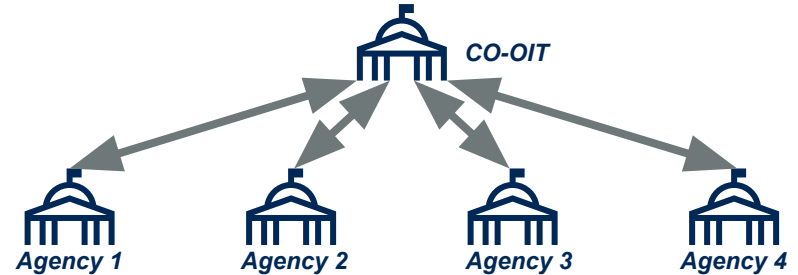
- Which PII Data elements are contained within this Entry/Exit Point?
- How much data is contained within this Entry/Exit Point?
- Which direction does PII data flow at this Entry/Exit Point?
- How often does this specific flow of data occur?
- What is the format the data is contained with?
- Is there a Data Sharing Agreement in place which governs this Entry/Exit Point?
- Does the Data Sharing Agreement indicate all the PII data elements which are contained within this Entry/Exit Point?

Implementation and Roles

CO-OIT can either collaborate with Colorado Agencies or provide the necessary resource to conduct Data Risk Assessments

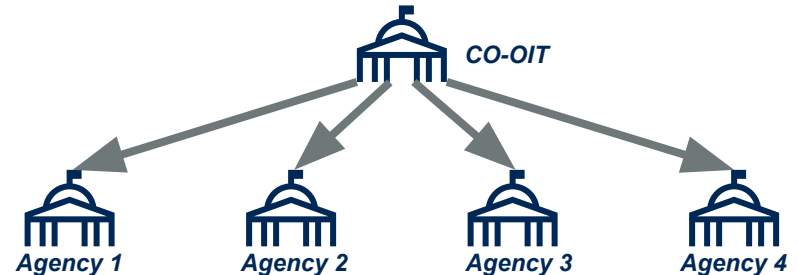
Scenario 1

- CO-OIT & Agencies will design Risk Assessment process and identify relevant business processes
- Conduct assessments with Agency and CO-OIT staff
- Consolidate assessment results and generate remediation steps based upon CO-OIT, Agency, & State Policy



Scenario 2

- CO-OIT designs Risk Assessment process and provides training to relevant Agency personnel.
- Agencies identify relevant business processes and conduct assessments
- Agencies consolidate assessment results and generate remediation steps based upon CO-OIT, Agency, & State Policy
- Agencies share findings with CO-OIT to ensure alignment to best practices and stated policies



Coordination among various OIT and agency personnel groups is critical to effectively implementing Data Risk Assessments within existing security processes

SP-05-191

OIT will require input from several roles within each agency to appropriately assess each business process and identify potential data risks. Various agency personnel groups can be included as part of the assessment interview process to provide insight or expertise for the business process in question.

These roles include but are not limited to:

| Role | Responsibility |
|---|---|
| <i>Business Process Manager/Owner</i> | Owner of the business process who operates and manages all the appropriate documentation. |
| <i>Business Process SME</i> | Individuals who conduct the business process who can offer expertise for specific tasks or systems |
| <i>Application/System Managers</i> | Individuals responsible for the maintenance and operation of applications/systems which are incorporated into business processes |
| <i>Technical/Security SMEs</i> | Individuals who are involved with the maintenance or operations of specific applications/systems or can provide expertise related to the security of those applications/systems |
| <i>Chief Information Security Office</i> | Office/individual who can provide expertise or insight into agency specific security regulations and policy pertaining to critical data |
| <i>Chief Privacy Office</i> | Office/individual who can provide expertise or insight into agency specific privacy regulations and policy pertaining to critical data |

Additional Considerations

Assessment M&O



- CO-OIT, Agencies and their IT Business Analysts must continue to collaborate on security assessment efforts.
- Educating future team members is critical to ensuring lasting integration into Colorado Agency operational processes and compliance.

Engaging IT Analysts



- IT Business Analysts are imperative to the success of critical data asset mapping.
- Colorado agencies must identify which IT business analysts or other personnel correspond to program areas within the organization to insure the constant upkeep of security assessment assets.

Change Management

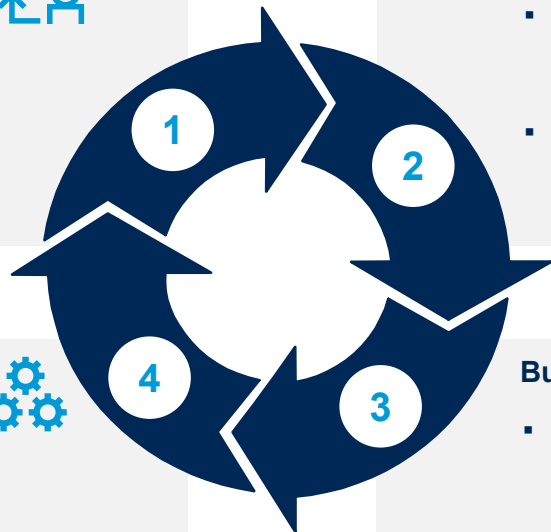


- Governance integration will require all processes to be controlled through change management procedures; therefore, providing thorough review and analysis of all recommended changes to prevent future risk exposure.

Business Process Ownership



- Business process owners must alert IT Business Analysts to any changes to operational procedures to ensure that they are captured correctly and then assessed appropriately.



Integrate the Security Assessment effort into the larger Change Management/Governance entities

In order for CalPERS to continue to evolve yet maintain strict security standards, the ability to rapidly change and incorporate security assessment findings is critical. The organizational must be able to quickly adapt to respond to potential threats or risks which are identified.

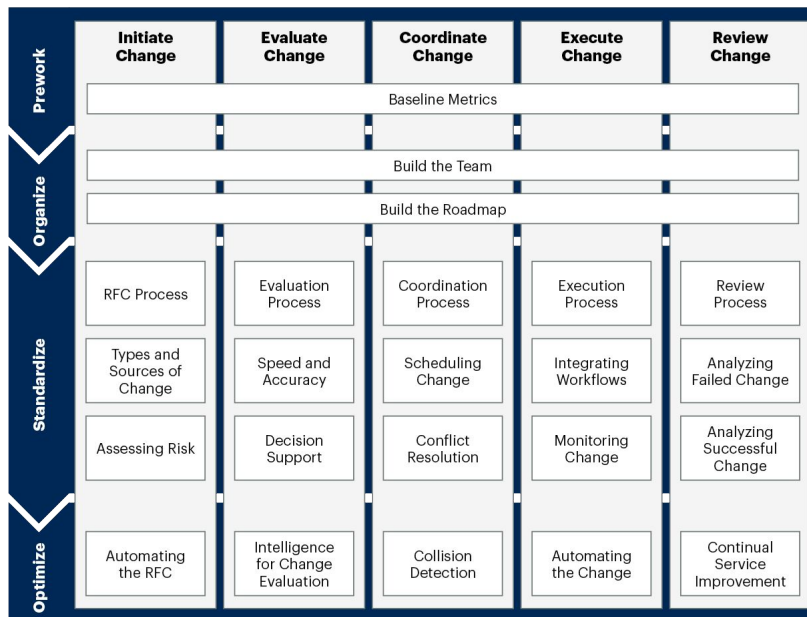
Evaluate existing change management processes, resources, and tools to identify potential change inputs.

Isolate process connections, overlaps, and similarities between the Security Assessment outputs and change management requirements.

Optimize IT/Security service delivery by integrating change management with adjacent ITSM and IT operations management (ITOM) workflows. Bring together data from security assessments and additional sources to enhance decision support for change evaluation, coordination, and review.

Create collaborative teams which include change management, ITSB, ISOF, and Program Area personnel to promote communication for proposed changes.

Change Management Framework



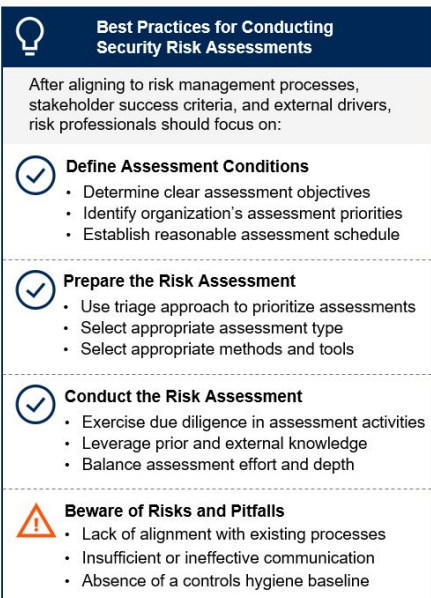
Source: Gartner
720845_C

Source: How to Implement a Modern IT Change Management Practice, G00720845

Identify alternative methods to initiate PII or critical data asset mapping outside of compliance

- Most security risk assessments are aimed at compliance-driven exercises; the outcome of the assessment should be to achieve risk-based treatment decisions. Teams must focus on achieving that goal to add value to the business.
- Make sure that all risk assessments incorporate an enterprise standard likelihood and impact measurement methodology as a prerequisite. This avoids inconsistency in risk communication, acceptance and treatment requirements.
- Adopt basic IT security hygiene activities to establish baseline security controls without doing security risk assessments; do opt-out assessments instead.

Best-Practice Framework



Source: Gartner
ID: 439861

Source: *Best Practices for a Successful Security Risk Assessment*, G00439861

Appendix

There is an associated risk to PII data in an MDM system if appropriate data security controls are not put in place. To reduce this risk the State must develop an MDM strategy, which focuses on PII master data security for both PII data in motion and data at rest. The strategy should consider the following:

1

Leveraging application security provided by the MDM solution

Built-in solution security functionality can jumpstart the implementation of appropriate controls or restrictions for critical data elements

2

Assess, remediate and monitor sensitive data risks

Standardized policies for risk identification, management, and reporting will provide CO OIT increased insight into potential security incidents and ensure appropriate corrective actions are taken.

3

Collaborate with the State CISO to define data security policies

Garner input from security and data offices to ensure alignment with existing or upcoming policies or regulatory requirements.

Leveraging application security provided by the MDM solution

ESG 191

User Authentication

MDM solution must have a user authentication management protocol in place to ensure the user or application has the right access to log into the MDM solution

User Authorization

MDM solution must provide the ability to create role-based user or application authorizations enabling access of data needed to complete the tasks allowed by the user or application

Record Audit

MDM solution must provide an audit trail and time stamp capabilities. This will provide the State with the capability to see who has requested or accessed which PII MDM records, when and where. This will trigger alerts and workflows to flag unauthorized behavior.

RESTRICTED

Collaborate with the CISO to help define data and then implement data security policies and procedures

It is critical that data privacy policies are defined by the CISO with input from Data and Analytics leadership

01. Data Governance

- Guidelines, policies and standards to support data privacy and security
- Data cataloging
- Business Glossary
- Data Stewardship
- Data Lifecycle Management
- Data Usage / Data Sharing



02. Data Privacy

- Data Privacy Policies
- Federal and State Regulatory Requirements
- Federal and State Compliance Monitoring
- Data Classification

03. Data Security

- Data Access, Authorization, & Audit
- Data Security Tools and Resources
- Data Incident Reporting

Bharat Bagaria

Expert Partner
Gartner Consulting
Phone: +1 916 210 0907
Email: bharat.bagaria@gartner.com

Chelsea Wyatt

Senior Managing Partner
Gartner Consulting
Phone: +1 303 590 8599
Email: chelsea.wyatt@gartner.com

Farhat Naweed

Senior Director
Gartner Consulting
Phone: +1 475 685 5848
Email: farhat.naweed@gartner.com

Nikhil Nayak

Associate Director
Gartner Consulting
Phone: +1 916 213 7447
Email: nikhil.nayak@gartner.com

Lauren Talyor

Account Executive
Gartner
Phone: +1 205 837 3693
Email: lauren.talyor@gartner.com

PII Data Management Program: Initiative Roadmap

Prepared for OIT
15th December 2022
Gartner Engagement #330079673



Contents

162 of 191



01

Initiative Roadmap Overview

Pages 3 – 6



02

Data Management Program: Roadmap Initiative Details

Pages 7 – 33

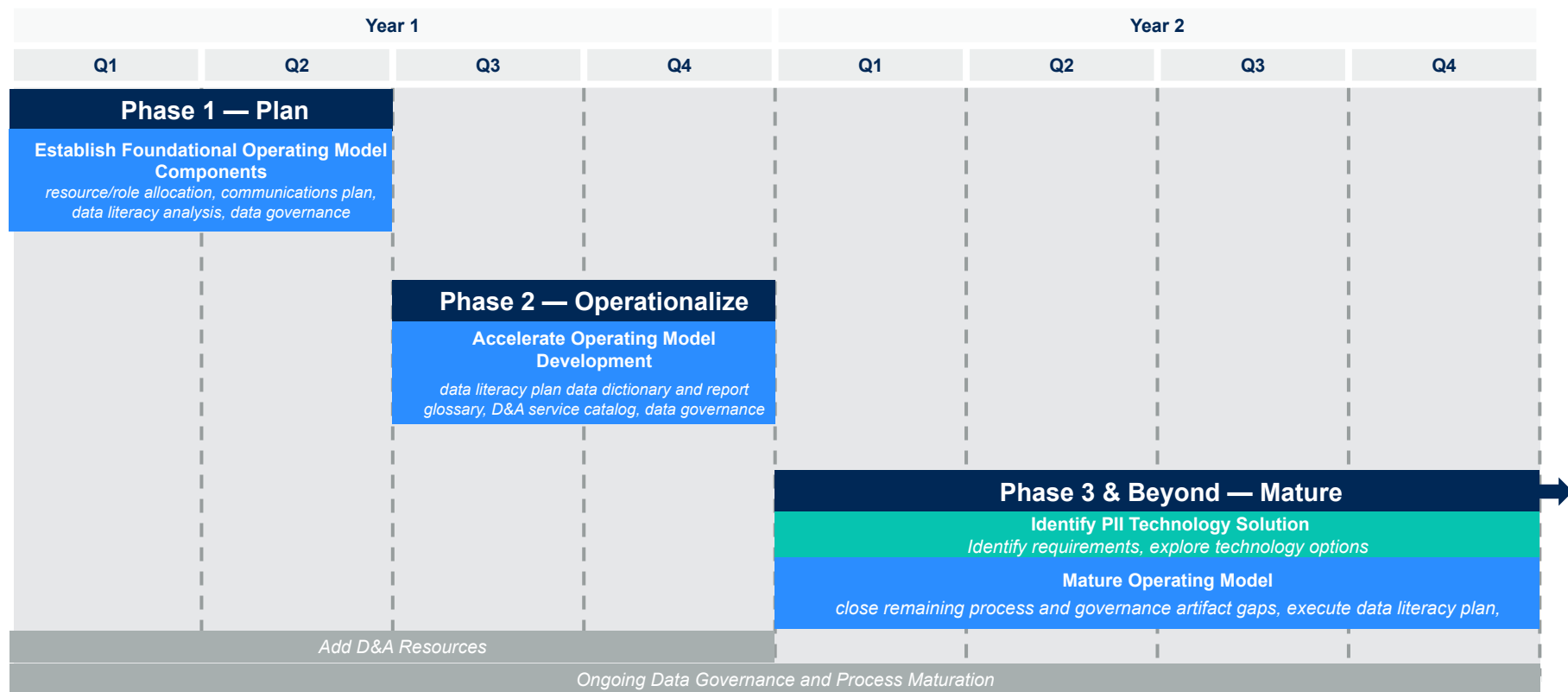
RESTRICTED

162 © 2021 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

Overview

D&A Implementation Roadmap — Multiple Phase Approach ^{*}164 of 191

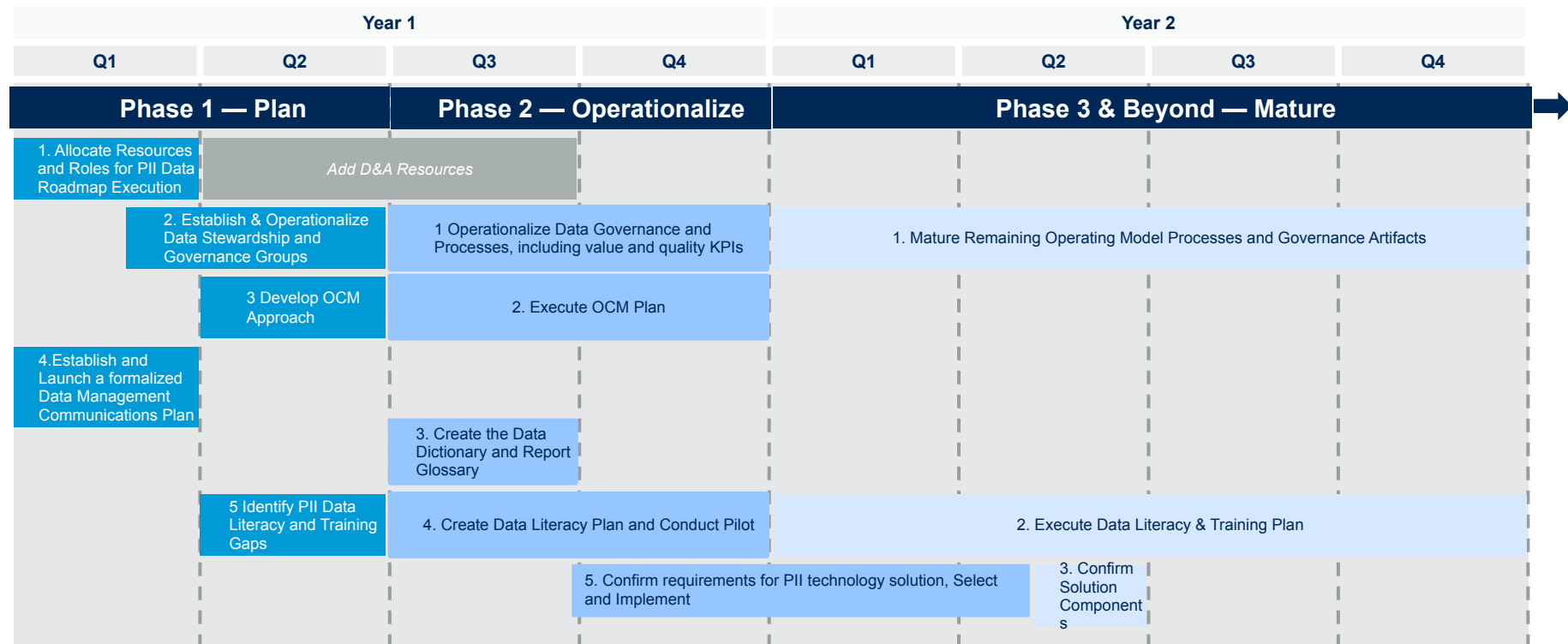


^{*}Assumes 100% OIT Effort

RESTRICTED

D&A Implementation Roadmap — Detail View

165 of 191



RESTRICTED

D&A Implementation Roadmap — Activities and Outcomes 166 of 191

Phase 1 – Plan

1. Allocate Resources and Roles for PII Data Roadmap Execution
2. Establish & Operationalize Data Stewardship and Governance Groups
3. Develop OCM Approach
4. Create D&A Communications Plan
5. Identify PII Data Literacy and Training Gaps

Phase 2 — Operationalize

1. Operationalize Data Governance and Processes, including value and quality KPIs
2. Execute OCM Plan
3. Create the Data Dictionary and Report glossary
4. Create Data Literacy Plan and Conduct Pilot
5. Confirm requirements for PII technology solution, Select and Implement

Phase 3 & Beyond – Mature

1. Mature Remaining Operating Model Processes and Governance Artifacts
2. Execute Data Literacy & Training Plan
3. Confirm solution components

Outcomes

- Defined D&A roles and responsibilities across the OIT IT and Business Partners
- An operational data Governance council and defined playbook for a roster of data stewards
- OCM Team and Change Plan is established
- Communication Plan is defined
- Establish the foundation for PII data literacy

Outcomes

- Operationalize data governance hence ensuring data is accessible and protected
- Executing OCM to reduce departmental resistance and ensuring the changes are implemented and sustained successfully.
- Data Literacy Planed and pilot is completed

Outcomes

- Steady refinement and maturation of the operating, process and governance models over time
- Data Literacy Learning Plans are in place and getting executed on regular basis
- Resources allocated to support the PII technology solution

Phase 1 — Plan

Phase 1 Step 1: Allocate Resources and Roles for PII Data Management Roadmap Execution 168 of 191

| <div>Overview</div> <div><ul style="list-style-type: none">This step will focus on establishing a plan to fulfill the needed functional resources to deliver the support required for the management of the PII Data Management Roadmap..</div> | <div>Business Benefits/Outcomes</div> <div><ul style="list-style-type: none">As a key dependency for program advancement, the resourcing plan will be a critical point to reflect executive support and investment in moving forward.The creation of new and/or modified Data Management roles will open career opportunities for current staff interested in advancement.</div> | <div>Primary Owner(s)</div> <div>CDO, GDAB</div> <div>Estimated Core Work Effort</div> <div>3 months</div> <div>Dependencies</div> <div><ul style="list-style-type: none">N/A</div> | | | | | | |
|--|---|---|----------------|---------------------|--|---|---|--|
| <div>Execution Guidance and Assumptions</div> <div><ul style="list-style-type: none">Establishing funding and executing the hiring process for various staff roles will take time. It will be possible to make progress on roadmap phases 1 and 2 (albeit more slowly) with current resources assuming adjustments to current responsibilities.Staff augmentation or consulting assistance could also be pursued to expedite progress while hiring for key roles.</div> | <table><tr><th>Key Activities</th><th>Description</th></tr><tr><td>1. Create staffing plan</td><td><div><input type="checkbox"/> Assess the role gaps required to execute the roadmap and ongoing D&A operations</div><div><input type="checkbox"/> Consider existing resources to determine where gaps can be addressed.</div><div><input type="checkbox"/> Determine a prioritized list of positions (starting with roadmap phase 1 &2) required and prepare funding request</div></td></tr><tr><td>3. Create hiring plan to staff needs for phase 3 and beyond</td><td><div><input type="checkbox"/> Determine the positions required to close gaps in roles and responsibilities to mature and execute the new operating model long term</div><div><input type="checkbox"/> Execute hiring plan</div></td></tr></table> | | Key Activities | Description | 1. Create staffing plan | <div><input type="checkbox"/> Assess the role gaps required to execute the roadmap and ongoing D&A operations</div> <div><input type="checkbox"/> Consider existing resources to determine where gaps can be addressed.</div> <div><input type="checkbox"/> Determine a prioritized list of positions (starting with roadmap phase 1 &2) required and prepare funding request</div> | 3. Create hiring plan to staff needs for phase 3 and beyond | <div><input type="checkbox"/> Determine the positions required to close gaps in roles and responsibilities to mature and execute the new operating model long term</div> <div><input type="checkbox"/> Execute hiring plan</div> |
| Key Activities | Description | | | | | | | |
| 1. Create staffing plan | <div><input type="checkbox"/> Assess the role gaps required to execute the roadmap and ongoing D&A operations</div> <div><input type="checkbox"/> Consider existing resources to determine where gaps can be addressed.</div> <div><input type="checkbox"/> Determine a prioritized list of positions (starting with roadmap phase 1 &2) required and prepare funding request</div> | | | | | | | |
| 3. Create hiring plan to staff needs for phase 3 and beyond | <div><input type="checkbox"/> Determine the positions required to close gaps in roles and responsibilities to mature and execute the new operating model long term</div> <div><input type="checkbox"/> Execute hiring plan</div> | | | | | | | |
| <table><tr><th>Key Risk</th><th>Mitigation Strategy</th></tr><tr><td>Limited internal resources to meet the PII Data Management roadmap needs</td><td><div><ul style="list-style-type: none">Look for potential partners to close the resource and skills gapsExplore how responsibilities for current roles can be adjusted to begin roadmap advancement.</div></td></tr></table> | | | Key Risk | Mitigation Strategy | Limited internal resources to meet the PII Data Management roadmap needs | <div><ul style="list-style-type: none">Look for potential partners to close the resource and skills gapsExplore how responsibilities for current roles can be adjusted to begin roadmap advancement.</div> | | |
| Key Risk | Mitigation Strategy | | | | | | | |
| Limited internal resources to meet the PII Data Management roadmap needs | <div><ul style="list-style-type: none">Look for potential partners to close the resource and skills gapsExplore how responsibilities for current roles can be adjusted to begin roadmap advancement.</div> | | | | | | | |

Phase 1 Step 2: Establish & Operationalize Data Stewardship and Governance Groups

| | | | | |
|---|--|---|--|--|
| Overview <ul style="list-style-type: none">This initiative focuses on designing and implementing the appropriate Data & Analytics governing committee and its ways of working with the other governing committees.This initiative also formalizes and communicates the Data Steward and Owner roles from the Departments.This initiative also establishes the Terms of Reference for Data Governance, ensuring clear scope of responsibilities and decision requirements for the Data & Analytics governing bodies | | Business Benefits/Outcomes <ul style="list-style-type: none">Enables OIT to ensure that impactful investments are made, data policies and controls are implemented, high data literacy exists, and the benefits of treating data as an enterprise asset are communicatedDocuments the measurable benefits of the use of PII data across the State of Colorado DepartmentsImplements adaptive data governance and policies based on the importance and sensitivity of the data assets in question | | Primary Owner(s) Data Governance Lead, CDO, GDAB |
| | | | | Estimated Core Work Effort 3-6 months, with ongoing management |
| | | | | Dependencies <ul style="list-style-type: none">Phase 1 Step 1: Allocate Resources and Roles for PII Data Management Roadmap Execution |
| Execution Guidance and Assumptions <ul style="list-style-type: none">Involve data domain experts from the Departments to function as Data Stewards and Owners | | | | |
| Key Risk | | Mitigation Strategy | | |
| Lack of organizational commitment | | <ul style="list-style-type: none">Ensure there is a clear purpose and scope for governance groups with the appropriate decision makers who have a vested interest in data governanceEstablish organizational mandate for a data-driven culture | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Phase 1 Step 3: Develop OCM Approach

170 of 191

| | | | | |
|---|--|--|--|---|
| Overview <ul style="list-style-type: none"> This initiative focuses on establishing and operationalizing an Organization Change Management (OCM) approach to get OIT ready for the change associated with executing the PII Data Management roadmap initiatives Benefiting from data requires users to change the way they do their jobs. A clear and consistent OCM plan should be developed to raise the Departments' understanding of the change impacts. The plan should incorporate the artifacts such as user guides, training and knowledge transfer plans, communication strategy, readiness assessment. | | Business Benefits/Outcomes <ul style="list-style-type: none"> Strengthens buy in with in the individual departments for the PII Data Management approach Improves business transparency into what OIT has in store today and what is planned Prepares the individual departments in advance of the changes being implemented Drives the individual departments to adopt a change adaptive culture | | Primary Owner(s) Change Management Lead |
| Execution Guidance and Assumptions <ul style="list-style-type: none"> The OCM plan should include the following: <ul style="list-style-type: none"> Change Management Impacts User Guide Creation/Changes Training Knowledge Transfer Executive and stakeholder engagement plans Assess readiness in each unit to determine necessary mitigation strategies | | Estimated Core Work Effort 3-6 months plus ongoing management | | Dependencies <ul style="list-style-type: none"> Phase 1 Step 1: Allocate Resources and Roles for PII Data Roadmap Execution Phase 1 Step 2: Establish & Operationalize Data Stewardship and Governance Groups |
| Key Risk Enterprise alignment, adoption and culture change | | Mitigation Strategy <ul style="list-style-type: none"> OCM activities relating to PII data should be coordinated and aligned with the PII Data Management communication plan. Impacted stakeholders should be well informed during the entire process to drive buy in and acceptance | | Key Activities <ol style="list-style-type: none"> Identify the business changes due to changes to the governance and management of PII data <ul style="list-style-type: none"> Identify the business changes and stakeholders impacted Establish OCM Team (and training needs) Schedule change management meetings to discuss the changes needed to implement identified changes Create a change management timeline with detailed activities Create Training Plan <ul style="list-style-type: none"> Develop the training plan, including for new technologies that may be incorporated Tailor learning paths to the respective stakeholder groups based on readiness assessment and communicate as needed Receive feedback from individual departments on training Iteratively improve future training details, style and frequency that are preferred and required Create Knowledge Transfer Plan <ul style="list-style-type: none"> Develop the knowledge transfer plan Receive feedback from individual departments on knowledge transfer Iteratively improve future knowledge transfer details, style and frequency that are preferred and required |
| Description | | | | |

RESTRICTED

Phase 1 Step 4 : Establish and Launch a formalized Data Management Communications Plan


171 of 191

| Overview | |
|--|---|
| <ul style="list-style-type: none">▪ This initiative focuses on establishing and operationalizing a communication plan to make the enterprise aware of the plans, objectives, services and value that PII Data Management offers.▪ Benefiting from PII data security and usage requires users to change the way they do their jobs. A clear and consistent message should be developed to raise each department's understanding of the opportunities, success stories and benefits gained from using / sharing PII data. | |
| Execution Guidance and Assumptions | |
| <ul style="list-style-type: none">▪ The communications plan should include the following:<ul style="list-style-type: none">– Key Messages– Audiences and their Key Issues– Messages by Audience including benefits/value, metrics, etc.– Media used to communicate– Action plans (e.g., milestones, action items, responsibilities)– Feedback loops to capture the effectiveness of communication. | |
| Key Risk | |
| Enterprise alignment | <ul style="list-style-type: none">▪ Executive / enterprise communications and actions relating to PII data and analytics should be coordinated and aligned with the Data Management communication plan. |

| Business Benefits/Outcomes | |
|--|--|
| <ul style="list-style-type: none">▪ Informs the individual State of Colorado Departments of how PII Data Management objectives are tied to the HD 21-1111 and other State and Federal Statutes and policies.▪ Strengthens PII Data Management program buy-in from the individual departments▪ Improves business transparency into what PII Data Management has in store today and what is planned for the future | |

| Primary Owner(s) | |
|---|--|
| Change Management Lead | |
| Estimated Core Work Effort | |
| 3 months plus ongoing management | |
| Dependencies | |
| <ul style="list-style-type: none">• N/A | |

| Key Activities | | Description | |
|--|--|-------------|--|
| 1. Identify target audiences and preferred communication methods | <ul style="list-style-type: none"><input type="checkbox"/> Identify stakeholder segments (may be done through personas) to receive communications from OIT and GDAB<input type="checkbox"/> Determine the communication methods by which targets audiences will prefer to receive communications (e.g., email, conference call, in-person meeting). | | |
| 2. Create communication plan and deliver communications | <ul style="list-style-type: none"><input type="checkbox"/> Develop the communications plan.<input type="checkbox"/> Tailor education, and communication materials to the respective stakeholder groups and communicate as needed. | | |
| 3. Iteratively improve communication | <ul style="list-style-type: none"><input type="checkbox"/> Receive feedback from the stakeholder groups on communications.<input type="checkbox"/> Iteratively improve future communication details, style and frequency that are preferred and required. | | |



Phase 1 Step 5: Identify PII Data Literacy and Training Gaps

172 of 191

| Overview <ul style="list-style-type: none">▪ This initiative focuses on understanding and documenting the current state, and the desired future state for PII data literacy within the OIT, the individual departments and external data consumer community.▪ Identification of important PII data literacy and training gaps in this step will feed future steps of the roadmap.▪ It is the first of a three-step approach across the three roadmap phases aimed at identifying, addressing, and closing PII data literacy gaps | | Business Benefits/Outcomes <ul style="list-style-type: none">▪ Current state identification conversations with partners will begin to build change awareness and identify appetites for participation and champions within business areas.▪ Identification of current state literacy deficiencies will inform training content and methods required to have an impact in future phases. | | Primary Owner(s) <div>Training Lead</div> Estimated Core Work Effort <div>3-5 months</div> Dependencies <ul style="list-style-type: none">• Phase 1 Step 1: Allocate Resources and Roles for PII Data Roadmap Execution• Phase 1 Step 2: Establish & Operationalize Data Stewardship and Governance Groups• Phase 1 Step 3: Develop OCM Approach | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---------------------|---|---|--|--|--|--|----------------|--|-------------|--|---|--------------------------|---|--|--|--------------------------|---|--|--------------------|--------------------------|--|--|--|--------------------------|--|--|------------------------|--------------------------|--|--|
| Execution Guidance and Assumptions <ul style="list-style-type: none">▪ Business users may be familiar with the GDAB definition of PII data. Consideration should be given to how the definition diverges from the GDAB definition when combined with departmental data | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table><tr><th>Key Risk</th><th>Mitigation Strategy</th></tr><tr><td>Lack of Participation</td><td><ul style="list-style-type: none">▪ Executive leadership should communicate directly about the importance of participation including benefits for key roles that frequently rely on PII data.</td></tr></table> | | Key Risk | Mitigation Strategy | Lack of Participation | <ul style="list-style-type: none">▪ Executive leadership should communicate directly about the importance of participation including benefits for key roles that frequently rely on PII data. | <table><tr><th colspan="2">Key Activities</th><th colspan="2">Description</th></tr><tr><td>1. Executive communication about the initiative</td><td><input type="checkbox"/></td><td colspan="2">Initiate executive communication about the change initiative and the benefits to data users for improving their PII data literacy and becoming more skilled in analytics tools.</td></tr><tr><td>2. Determine the data literacy current state</td><td><input type="checkbox"/></td><td colspan="2">Conduct interviews of internal and external partners to establish a baseline of the current state of data literacy.</td></tr><tr><td>3. Assess the gaps</td><td><input type="checkbox"/></td><td colspan="2">Identify PII data literacy gaps that must be addressed through training.</td></tr><tr><td>4. Assess current training and documentation</td><td><input type="checkbox"/></td><td colspan="2">Assess the current state of any PII data literacy trainings and documentation to inventory any currently developed assets.</td></tr><tr><td>5. Synthesize findings</td><td><input type="checkbox"/></td><td colspan="2">Synthesize findings from analysis into identifiable and documented PII data literacy and training gaps</td></tr></table> | | | | Key Activities | | Description | | 1. Executive communication about the initiative | <input type="checkbox"/> | Initiate executive communication about the change initiative and the benefits to data users for improving their PII data literacy and becoming more skilled in analytics tools. | | 2. Determine the data literacy current state | <input type="checkbox"/> | Conduct interviews of internal and external partners to establish a baseline of the current state of data literacy. | | 3. Assess the gaps | <input type="checkbox"/> | Identify PII data literacy gaps that must be addressed through training. | | 4. Assess current training and documentation | <input type="checkbox"/> | Assess the current state of any PII data literacy trainings and documentation to inventory any currently developed assets. | | 5. Synthesize findings | <input type="checkbox"/> | Synthesize findings from analysis into identifiable and documented PII data literacy and training gaps | |
| Key Risk | Mitigation Strategy | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Lack of Participation | <ul style="list-style-type: none">▪ Executive leadership should communicate directly about the importance of participation including benefits for key roles that frequently rely on PII data. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Key Activities | | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. Executive communication about the initiative | <input type="checkbox"/> | Initiate executive communication about the change initiative and the benefits to data users for improving their PII data literacy and becoming more skilled in analytics tools. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2. Determine the data literacy current state | <input type="checkbox"/> | Conduct interviews of internal and external partners to establish a baseline of the current state of data literacy. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3. Assess the gaps | <input type="checkbox"/> | Identify PII data literacy gaps that must be addressed through training. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4. Assess current training and documentation | <input type="checkbox"/> | Assess the current state of any PII data literacy trainings and documentation to inventory any currently developed assets. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5. Synthesize findings | <input type="checkbox"/> | Synthesize findings from analysis into identifiable and documented PII data literacy and training gaps | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |



Phase 2 — Operationalize

Phase 2 Step 1: Execute OCM Plan

174 of 191

| | | | | |
|---|--|---|--|--|
| Overview <ul style="list-style-type: none">This initiative focuses on executing the organization change management plan for PII Data by providing the necessary training and procedure updates to the impacted stakeholders and end users. | | Business Benefits/Outcomes <ul style="list-style-type: none">Strengthens PII Data program buy-in from each stakeholder groupImproves business transparency into what PII Data Management has in store today and what is plannedPrepares the team in advance of the changes being implementedDrives the workforce to be more adaptive to culture changes | | Primary Owner(s) Change Management Analyst, Training Lead |
| Execution Guidance and Assumptions <ul style="list-style-type: none">The OCM plan should focus on the training needs based on each department and their specific use cases | | Estimated Core Work Effort 3-6 months plus ongoing management | | Dependencies <ul style="list-style-type: none">Phase 1 Step 3: Develop OCM Approach |
| Key Risk Enterprise adoption and culture change | | Mitigation Strategy <ul style="list-style-type: none">Impacted stakeholders should be well informed during the entire process to drive buy in and acceptanceExecutive support for new operating model needs to be continuously promoted | | |
| Key Activities | | Description | | |
| 1. Implement the business changes due to PII Data | | <input type="checkbox"/> Implement the necessary business changes due to PII Data Management Policies, Processes and the potential introduction of new technology implementations | | |
| 2. Conduct Training for stakeholder groups | | <input type="checkbox"/> Deliver the training plan for each department / stakeholder group <input type="checkbox"/> Receive feedback from each department / stakeholder group on training <input type="checkbox"/> Iteratively improve future training details, style and frequency that are preferred and required | | |

Phase 2 Step 2: Operationalize Data Governance and Processes, including value and quality KPIs ¹⁹

| | | | | | |
|--|--|---|--|---|--|
| Overview | | Business Benefits / Outcomes | | Primary Owner(s) | |
| <ul style="list-style-type: none">This initiative focuses on designing and implementing the appropriate Data Management governing bodies at each of the departments and validate the role of GDABThis initiative also establishes the Terms of Reference for Data Governance, ensuring clear scope of responsibilities and decision requirements for the Data Management governing bodies at the department level and OITFinally, this initiative assumes the responsibility for the development and population of data value and quality KPIs | | <ul style="list-style-type: none">Enables OIT to ensure that high data quality exists, that impactful investments are made, that data policies and controls are implemented, and that the benefits of treating data as an enterprise asset are communicatedDocuments the measurable benefits of the use of data across the State DepartmentsImplements adaptive data governance and policies based on the importance and sensitivity of the data assets in question | | CDO | |
| Execution Guidance and Assumptions | | | | Estimated Core Work Effort | |
| <ul style="list-style-type: none">Integrate efforts with Information Security to liaise on data sensitivity parameters and policiesInvolve data domain experts from the Programs to function as data Stewards | | | | 9 months, with ongoing management | |
| | | | | Dependencies | |
| | | | | <ul style="list-style-type: none">N/A | |
| | | Key Activities | | Description | |
| | | 1. Design Data Management governing bodies | | <ul style="list-style-type: none">OIT to support establishing Charter and terms of reference for each of the department governing bodies.Begin holding governance discussions / meetings (e.g., begin developing and approving key governance artifacts / make key governance decisions).Establish a mechanism for feedback on how governance groups are operating and continuously improve. | |
| | | 2. Identify and deploy stewardship roles | | <ul style="list-style-type: none">Define domains and subdomains.Identify lead (and data stewards) by data domain and subdomain.Develop role descriptions and incentives with help of HR.Document individuals in a data steward roster.Create / Update the Data Governance charter to reflect Steward membership.Develop Stewardship playbook highlighting responsibilities, processes, resources, etc.Train and deploy data stewards. | |
| | | 3. Define Data Management Value and Quality KPIs | | <ul style="list-style-type: none">Define KPI metrics based on GDAB PII Data DefinitionsSocialize and communicate proposed metrics with key leaders. | |
| | | 4. Develop and publish Data Management KPIs | | <ul style="list-style-type: none">Develop a balanced scorecard based on defined KPIs.Publish the balanced scorecard based on a defined cadence.Communicate KPIs and establish mechanism for continuous feedback. | |
| Key Risk | | Mitigation Strategy | | | |
| Lack of organizational commitment | | <ul style="list-style-type: none">Leverage an executive level “champion” to advocate for Data Management.Ensure there is a clear purpose and scope for governance groups with the appropriate decision makers who have a vested interest in data management | | | |

175© 2021 Gartner, Inc. and/or its affiliates. All rights reserved.

Phase 2 Step 3: Create the Data Dictionary and Report glossary

176 of 191

| | | | | |
|---|--|--|--|--|
| Overview <ul style="list-style-type: none">▪ This initiative closes key Data governance artifact gaps by creating the Data Dictionary and Report glossary.▪ This is a widely accessible document that lists PII data assets and reporting along with detailed descriptions of the data, business rules / statutes governing its use and points of contact for the data (either a location where it can be found, a link to the data itself or a representative that can be reached for issues with the data). | | Business Benefits/Outcomes <ul style="list-style-type: none">▪ Creates a standard definition for each data element to maintain consistency across each of the departments▪ Improved use and understanding of available standard reports to both enable those in need of insights and relieve repetitive inquiries to the data team for content already available within standard reports.▪ Promoting data literacy by reducing variability and providing documentation resources to guide independent use | | Primary Owner(s) <p>Data Architect, Database Administrator, Data Owners</p> |
| Execution Guidance and Assumptions <ul style="list-style-type: none">▪ The Data and Report Glossary should be developed in conjunction with Business / Department representatives, be readily understood by business users and easy to find, access and navigate.▪ A clear process should be established for the addition of new data and reports. | | Estimated Core Work Effort <p>3-4 months</p> | | Dependencies <ul style="list-style-type: none">▪ Phase 1 Step 1: Allocate Resources and Roles for D&A Roadmap Execution▪ Phase 1 Step 2: Establish & Operationalize Data Stewardship and Governance Groups |
| Key Risk <p>Lack of refresh</p> | | Mitigation Strategy <ul style="list-style-type: none">▪ Once established, the data dictionary and report glossary can easily become dismissed as out-of-date if it is not updated regularly in conjunction with the addition of new data and reports. Refreshing the data dictionary should be a required step for any project that incorporates new data or creates new tables/reports. | | |
| Key Activities | | Description | | |
| 1. Catalog data elements | | <ul style="list-style-type: none"><input type="checkbox"/> Capture the names, definitions and attributes about each PII data element<input type="checkbox"/> Validate the list with stake-holding groups<input type="checkbox"/> Publish the list in an accessible location<input type="checkbox"/> Establish a process for operationally maintaining the dictionary including responsibilities for each role involved in the process | | |
| 2. Inventory standard data reports | | <ul style="list-style-type: none"><input type="checkbox"/> Compile a list of all current standard reports that use PII data<input type="checkbox"/> Validate the list with various stakeholders<input type="checkbox"/> Establish a process for operationally maintaining the report glossary and adding new reports as they are created<input type="checkbox"/> Publish the glossary in a location that is accessible by those who need access | | |

Phase 2 Step 4: Create Data Literacy Plan and Conduct Pilot

177 of 191

| | | | | |
|---|--|--|--|--|
| Overview <ul style="list-style-type: none"> This initiative focuses on establishing a formalized data literacy program to drive a data driven culture across the Departments It establishes a Data & Analytics Community of Practice and a standard collaboration platform for data users and producers to share insights and best practices further advancing PII data literacy | | Business Benefits/Outcomes <ul style="list-style-type: none"> Establishes a user classification and persona driven data literacy and training program for Data & Analytics stakeholders Builds up a knowledge repository over time accelerating Data & Analytics initiatives and sustainment with decentralized groups Fosters a user community with a desire to advance Data & Analytics capabilities | | Primary Owner(s) Training Lead |
| Execution Guidance and Assumptions <ul style="list-style-type: none"> Business users may be familiar with the GDAB definition of PII data. Consideration should be given to how the definition diverges from the GDAB definition when combined with departmental data | | Estimated Core Work Effort 6 months | | Dependencies <ul style="list-style-type: none"> Phase 1 Step 5: Identify Data Literacy and Training Gaps |
| Key Risk Training participation | | Mitigation Strategy <ul style="list-style-type: none"> Executive leadership should mandate PII data literacy training for any roles that uses data in decision making. | | |
| Key Activities | | Description | | |
| 1. Data literacy training design | | <input type="checkbox"/> Develop user personas around which to design data literacy initiatives <input type="checkbox"/> Develop training structure, content, and cadence based on user personas <input type="checkbox"/> Run a pilot program with a small group to understand what works and fine-tune the training processes, scaling when appropriate | | |
| 2. Continuous baselining and benchmarking data literacy | | <input type="checkbox"/> Define data literacy KPIs <input type="checkbox"/> Baseline and benchmark data literacy before and after first training initiative <input type="checkbox"/> Continue to evaluate training effectiveness and re-baseline as data literacy improves | | |
| 3. Compile collaboration platform requirements | | <input type="checkbox"/> Capture the core collaboration platform requirements <input type="checkbox"/> Select the right knowledge management/collaboration tooling through a hands-on evaluation process <input type="checkbox"/> Implement and deploy collaboration tool(s) | | |
| 4. Establish a Data & Analytics Community of Practice | | <input type="checkbox"/> Define vision, purpose, guidelines, logistics, etc. for a Data & Analytics Community of Practice <input type="checkbox"/> Market and establish Data & Analytics Community of Practice membership <input type="checkbox"/> Establish mechanism for feedback and continuously evolve the community | | |

RESTRICTED

Phase 2 Step 5: Confirm requirement for PII Data Management solution, Select and Implement

| | | | | |
|--|--|---|--|---|
| Overview <ul style="list-style-type: none">This initiative assesses at the appropriate time the need for a purpose-built PII data management solution such as master data management (MDM), metadata management, combination of MDM, metadata management or entity resolution in combination with a metadata management solution to maintain PII data security and grow data quality levels | | Business Benefits / Outcomes <ul style="list-style-type: none">Ensures a high-quality single source of the truthThe selected solution can determine when a central master record should be updated or rejected when fed by a source system and assigned for quality improvement. | | Primary Owner(s) Training Lead |
| | | | | Estimated Core Work Effort 3 – 9 months |
| | | | | Dependencies <ul style="list-style-type: none">N/A |
| Execution Guidance and Assumptions <ul style="list-style-type: none">Monitor data quality KPIs to determine timing for this initiativeCreate user feedback mechanism to collect data conflict and quality issues for PII dataMaintain open dialogue with data integration team to identify ETL or other ingestion issues and constraints | | | | |
| Key Risk High Cost of PII Data Management solutions | | Mitigation Strategy <ul style="list-style-type: none">Many of these solutions bring additional, valuable functionality that could be used in other areas of the Data Program (e.g. Business Glossary, Data Dictionary, etc.) – the high implementation and licensing costs could be defrayed by identifying additional benefits beyond pure master data management rules | | |

| Key Activities | | Description |
|---|--|-------------|
| 1. Identify and confirm cases of PII data conflicts and challenges | <input type="checkbox"/> Add PII data conflicts to Data Steward cadence <input type="checkbox"/> Monitor data feedback channel for PII data conflict <input type="checkbox"/> Maintain dialogue with data integration and EDW team | |
| 2. Determine ability of existing ingestion mechanisms to solve for complex data conflict and resolution | <input type="checkbox"/> Work with data integration team to assess effectiveness of current ingestion and integration tools <input type="checkbox"/> Identify specific areas of constraint | |
| 3. Quantify the costs of the data conflicts | <input type="checkbox"/> Work with data stewards and business stakeholders to identify cost of poor quality in master data | |
| 4. Research and investigate COTS MDM solutions | <input type="checkbox"/> Leverage independent research and advisory services to identify leading MDM and metadata management solutions and critical capabilities | |
| 5. Identify PII Data Management solution and build business case | <input type="checkbox"/> Build the business case, as required, to acquire the chosen PII data management solution and the range of functional capabilities they can bring to the State of Colorado. | |

RESTRICTED

Phase 3 & Beyond — Mature

Phase 3 Step 1: Mature Remaining Operating Model Processes and Governance Artifacts

| | | | | | |
|--|---|--|--|---|--|
| Overview <ul style="list-style-type: none">This initiative closes the remaining gaps in Data & Analytics processes and governance artifacts to achieve the objectives of the D&A program and the initiatives remaining in the Roadmap | | Business Benefits/Supported Goals <ul style="list-style-type: none">Improves the likelihood that D&A initiatives will be achieved within the timeframes laid out on the roadmap and sets OIT on a course towards continued operational excellence and delivering continuously improved business value | | Primary Owner(s) D&A Governance Lead, Data Stewards, Change Management Analyst, CDO | |
| Execution Guidance and Assumptions <ul style="list-style-type: none">Ensure OCM efforts continue throughout this journeyEstablish a defined location for storage of process and governance documents | | | | Estimated Core Work Effort 6-12 months and ongoing management | |
| | | | | Dependencies <ul style="list-style-type: none">Phase 1 Step 1: Allocate Resources and Roles for D&A Roadmap ExecutionPhase 2 Step 3: Create the Data Dictionary and Report glossaryPhase 2 Step 4: Create Data Literacy Plan and Conduct Pilot | |
| Key Risk | | Mitigation Strategy | | Key Activities | |
| Employee Turnover | <ul style="list-style-type: none">Begin cross pollination of skills and knowledge to reduce the impact of knowledge lostDocument all key artifacts to enable proper Knowledge transfer | | | Description | |
| Operational activities take precedent | <ul style="list-style-type: none">Schedule specific times for key individuals to review or complete next step actionsAssign ownership for continuous improvement activities beyond the initial document creation | | | | |
| | | | | 1. Review remaining D&A Process and Governance Artifacts gaps <ul style="list-style-type: none">Determine which gaps have been closed as a result of previous stepsDetermine if new gaps have emerged or been identifiedDocument remaining process and governance artifact gaps | |
| | | | | 2. Prioritize remaining D&A Process and Governance Artifacts gaps <ul style="list-style-type: none">Establish criteria for prioritizing remaining process and governance artifacts gapsPrioritize remaining process and governance artifacts gaps based on criteria linked to value driven use cases | |
| | | | | 3. Establish remaining D&A Processes and Governance Artifacts <ul style="list-style-type: none">Assign prioritized remaining D&A processes and governance artifacts to the responsible parties for development/establishmentResponsible parties create or update the respective D&A processes and governance artifactsNew processes and governance artifacts are documentedResponsible parties collaborate with Change Management Analyst to operationalize new processes and artifacts | |

Phase 3 Step 2: Execute Data Literacy & Training Plan

181 of 191

| | | | | |
|---|--|---|--|---|
| Overview <ul style="list-style-type: none">This initiative focuses on execution steps of a complete data literacy program to drive a data driven culture across the State of Colorado Departments. | | Business Benefits/Outcomes <ul style="list-style-type: none">Establishes a user classification and persona driven data literacy and training program for Data & Analytics stakeholders.Builds up a knowledge repository over time accelerating Data & Analytics initiatives and sustainment with decentralized groupsFosters a user community with a desire to advance OIT's Data and Analytics capabilities. | | Primary Owner(s) Training Lead |
| Execution Guidance and Assumptions <ul style="list-style-type: none">Understand stakeholder buy-in and leverage fast followers for initial training to gain momentum | | Estimated Core Work Effort Ongoing continuous management | | Dependencies <ul style="list-style-type: none">Phase 2 Step 4: Create Data Literacy Plan and Conduct Pilot |
| Key Risk Training participation | | Mitigation Strategy <ul style="list-style-type: none">Executive leadership should reinforce the need for data literacy training for any roles that make use of data in decision making. | | |
| Key Activities | | Description | | |
| 1. Iterate on Data Literacy & Training Pilot | | <ul style="list-style-type: none">Incorporate feedback and lessons learned from initial data literacy training pilot into enterprise-wide data literacy and training planEvaluate pilot based on established KPIsEvaluate initial performance of collaboration platform and address any identified improvementsLeverage the D&A Community of Practice and Change Management Analyst for preparation for enterprise-wide roll-out | | |
| 2. Execute Data Literacy & Training Plan | | <ul style="list-style-type: none">Communicate data literacy trainings and content based on user personasRun the trainings, continuously capturing and incorporating feedback | | |
| 3. Continuous baselining and benchmarking data literacy | | <ul style="list-style-type: none">Continue to calculate and monitor data literacy KPIsContinue to evaluate training effectiveness and re-baseline as data literacy improves. | | |

Phase 1 Step 7 : Confirm technology and partner selection process

182 of 191

| Overview <ul style="list-style-type: none">▪ This initiative determines how the initial tools and partners required for conducting a Proofs of Concept for a PII data management solution will be leveraged, acquired and evaluated▪ The objective for the Proof of Concept is to deliver observable business value, the tangible achievement of as many PII Data Management objectives as possible, and an illustration of how current state points can and will be addressed | | Business Benefits / Outcomes <ul style="list-style-type: none">▪ Documents and gains approval for selection processes that are potentially different than the way in which OIT has selected tools and partners in the past▪ Reduces the need to onboard all skills and roles as full-time equivalents if they can be rented on an interim basis from a partner | | Primary Owner(s) OIT, GDAB | | | | | | | | | | | | |
|--|--------------------------|---|--|--------------------------------------|----------------|--|-------------|--|--------------------------|--|--|--------------------------|---|--|--------------------------|---|
| Execution Guidance and Assumptions <ul style="list-style-type: none">▪ Confirm that tools and partner evaluation data is sufficiently available from sources other than the vendors themselves▪ Identify the risks and mitigation strategies of adopting a selection process that varies from the norm | | Estimated Core Work Effort 4 weeks | | Dependencies N/A | | | | | | | | | | | | |
| Key Risk Cost of an Unsuccessful Proof of Concept | | Mitigation Strategy <ul style="list-style-type: none">▪ Strive for a partner to put “skin in the game” as an indication of probability of success in the proof of concept and over the long-term▪ Structure payments based on the ability to implement the proof of concept in production▪ Take advantage of independent, expert advice on proof of concept finalists▪ Conduct reference checks on PoC finalists | | | | | | | | | | | | | | |
| | | Key Activities <table><tr><th colspan="2">Key Activities</th><th>Description</th></tr><tr><td>1. Identify Options for Tool and Partner Selection</td><td><input type="checkbox"/></td><td>Options could include RFI only, RFI followed by RFP, Sole Source, and Proof of Concept</td></tr><tr><td>2. Evaluate Pros and Cons of Selection Options</td><td><input type="checkbox"/></td><td>Articulate the costs, benefits, risks and mitigation strategies for the various Selection processes</td></tr><tr><td>3. Document Selection Options and Obtain Approval for non-Traditional Approaches</td><td><input type="checkbox"/></td><td>Package the Options in a document to obtain the necessary approvals and the conditions under which each Option can be leveraged</td></tr></table> | | | Key Activities | | Description | 1. Identify Options for Tool and Partner Selection | <input type="checkbox"/> | Options could include RFI only, RFI followed by RFP, Sole Source, and Proof of Concept | 2. Evaluate Pros and Cons of Selection Options | <input type="checkbox"/> | Articulate the costs, benefits, risks and mitigation strategies for the various Selection processes | 3. Document Selection Options and Obtain Approval for non-Traditional Approaches | <input type="checkbox"/> | Package the Options in a document to obtain the necessary approvals and the conditions under which each Option can be leveraged |
| Key Activities | | Description | | | | | | | | | | | | | | |
| 1. Identify Options for Tool and Partner Selection | <input type="checkbox"/> | Options could include RFI only, RFI followed by RFP, Sole Source, and Proof of Concept | | | | | | | | | | | | | | |
| 2. Evaluate Pros and Cons of Selection Options | <input type="checkbox"/> | Articulate the costs, benefits, risks and mitigation strategies for the various Selection processes | | | | | | | | | | | | | | |
| 3. Document Selection Options and Obtain Approval for non-Traditional Approaches | <input type="checkbox"/> | Package the Options in a document to obtain the necessary approvals and the conditions under which each Option can be leveraged | | | | | | | | | | | | | | |

Bharat Bagaria

Expert Partner
Gartner Consulting
Phone: +1 916 210 0907
Email: bharat.bagaria@gartner.com

Chelsea Wyatt

Senior Managing Partner
Gartner Consulting
Phone: +1 303 590 8599
Email: chelsea.wyatt@gartner.com

Farhat Naweed

Senior Director
Gartner Consulting
Phone: +1 475 685 5848
Email: farhat.naweed@gartner.com

Nikhil Nayak

Associate Director
Gartner Consulting
Phone: +1 916 213 7447
Email: nikhil.nayak@gartner.com

Lauren Talyor

Account Executive
Gartner
Phone: +1 205 837 3693
Email: lauren.talyor@gartner.com

[illegible]

[illegible]

[illegible]

[illegible]

[1] An individual responsible for definitions, policy, and practice decisions about data within their area of responsibility. For business data, the individual may be called a business owner of the data.

[2] A business leader and/or subject matter expert designated as accountable for: a) the identification of operational and business intelligence data requirements within an assigned subject area, b) the quality of data names, business definitions, data integrity rules, and domain values within an assigned subject area c) compliance with regulatory requirements and conformance to internal data policies and data standards, d) application of appropriate security controls,

[3] If applicable, include a contact who manages the technical execution of the database (e.g. database management, access and extraction).

[4] Describe what a single row in the data represents, as simply as possible

[5] If dataset lives in more than one system, use a separate row for each system.

[6] Examples of Cloud File Storage include Google Drive, Dropbox, etc.)

[7] How would you classify this data?

PUBLIC - this data could be publicly disseminated without any concerns;

PROTECTED - this data is protected by law or regulation and can only be shared or accessed internally and per organizational procedures; OR this information includes individually identified information;

[8] If you marked "Other" for Protected Data Classification, please indicate what law(s)/regulation(s) protect this data.

[9] Example: Education, Health, Member, Workforce